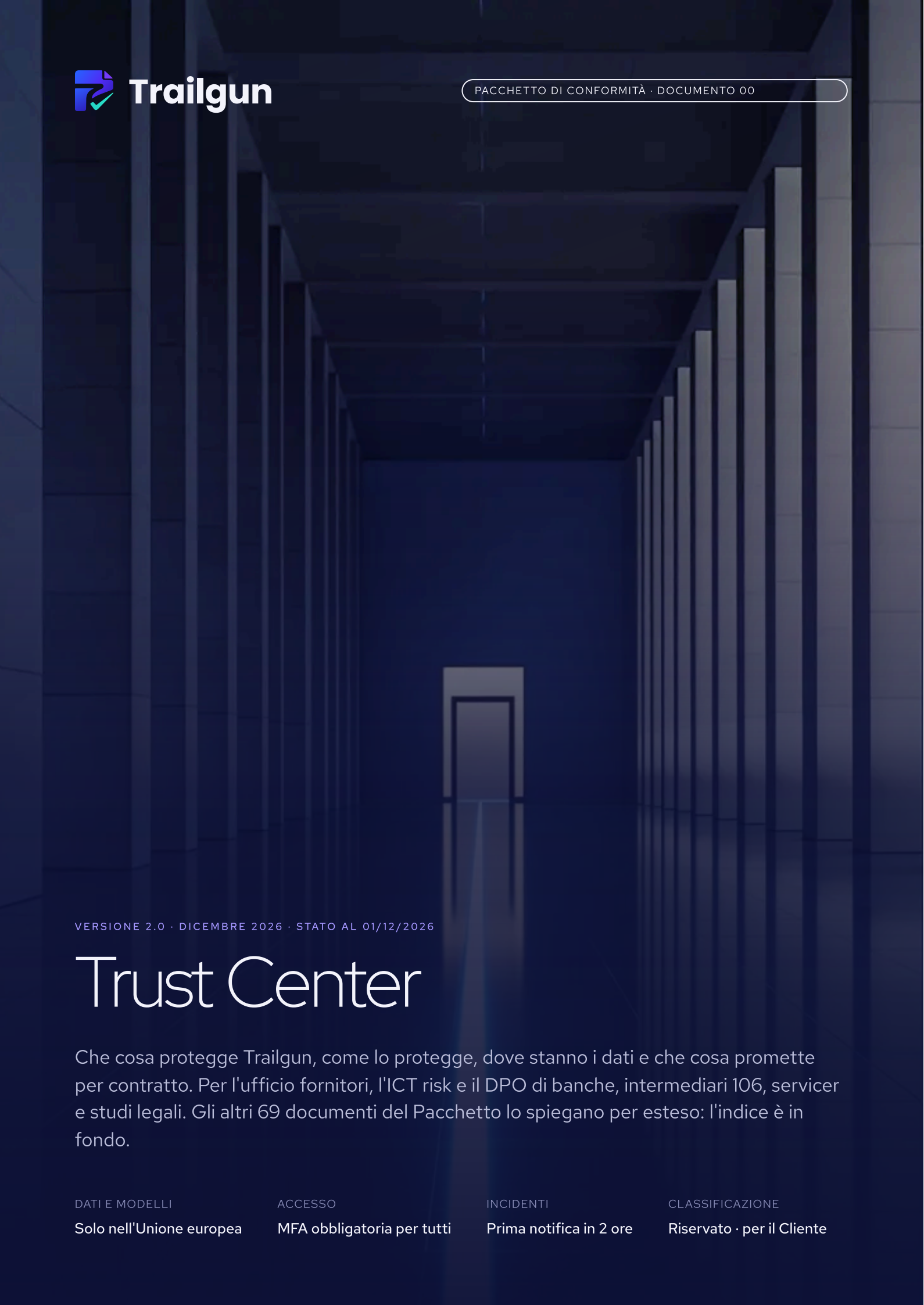
Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO 00



VERSIONE 2.0 · DICEMBRE 2026 · STATO AL 01/12/2026

Trust Center

Che cosa protegge Trailgun, come lo protegge, dove stanno i dati e che cosa promette per contratto. Per l'ufficio fornitori, l'ICT risk e il DPO di banche, intermediari 106, servicer e studi legali. Gli altri 69 documenti del Pacchetto lo spiegano per esteso: l'indice è in fondo.

DATI E MODELLI	ACCESSO	INCIDENTI	CLASSIFICAZIONE
Solo nell'Unione europea	MFA obbligatoria per tutti	Prima notifica in 2 ore	Riservato · per il Cliente

01 COSA PROTEGGIAMO

Le pratiche degli studi, con tutto ciò che contengono

Trailgun non è un assistente generalista: è una piattaforma a verticali. Agenti di intelligenza artificiale leggono l'archivio di una pratica e preparano atti, analisi e verifiche che un professionista rivede. Per farlo ricevono documenti tra i più delicati che esistano: crediti, garanzie, procedure concorsuali, fascicoli penali con intercettazioni.

4
canali d'ingresso: modulo, lotti, caselle email dedicate, API con chiavi dello studio

46
agenti di IA, su modelli Claude eseguiti in Amazon Bedrock nell'UE

2
regioni AWS dell'Unione: Francoforte per i dati, Irlanda per le copie

3
ambienti separati: development, staging, production

I verticali

- **Ricorso per decreto ingiuntivo**, dall'archivio del cliente al faldone pronto per il deposito.
- **Assessment**: questionari configurabili applicati a un faldone, come la due diligence sui crediti ceduti.
- **Insinuazione al passivo**, **escussione delle garanzie pubbliche** (Fondo PMI, SACE, ISMEA), **remediation del data tape** delle cartolarizzazioni.
- **Analisi del faldone**: relazione, domande con riferimento a documento e pagina, funzioni sul fascicolo penale, civile, amministrativo e tributario.
- **Trattative** sull'atto, a partire dall'affitto di ramo d'azienda.

I dati che riceviamo

- **Dati delle pratiche**: documenti e loro testo; anagrafiche di clienti, debitori, garanti e controparti; contratti, estratti conto, piani di ammortamento, garanzie; dati economici e fiscali.
- **Dati giudiziari**: atti di procedimenti civili, concorsuali, amministrativi, tributari e **penali** (art. 10 GDPR), comprese **intercettazioni e registrazioni audio**.
- **Elaborati**: atti, versioni, domande e risposte, conversazioni con gli agenti, email con i clienti dello studio.
- **Dati degli utenti e dello studio**: email, ruolo, preferenze; dati di fatturazione.
- **Dati tecnici**: log ed eventi di costo, senza testo dei documenti.

GDPR

Lo studio decide, Trailgun tratta

Lo studio, la banca o il servicer è titolare dei dati delle pratiche; Trailgun è responsabile del trattamento (art. 28) e li tratta solo su istruzione, con il DPA (documento 07; per gli studi legali il documento 04).

DORA

Fornitore terzo di servizi TIC

Art. 3, punto 19. Servizio «S19 Cloud services: SaaS» nel registro delle informazioni. Non è un fornitore critico designato. Per gli intermediari 106 si applica dal 1° gennaio 2027.

AI ACT

Fornitore del sistema

Trailgun è fornitore del sistema di IA; chi lo usa è deployer; Anthropic è fornitore del modello per finalità generali, eseguito da AWS. Nell'uso da parte di studi e servicer il sistema non è ad alto rischio.

Dati solo dallo studio

Arrivano dai canali dello studio; Trailgun non li raccoglie presso gli interessati.

Nessun addestramento

Né da Trailgun né dai fornitori dei modelli: lo dichiara il documento 60.

Nessun profilo

Le schede su una persona restano nella pratica; nessuna decisione automatizzata.

Nessun riuso tra clienti

Gli elaborati, le cache e le regole di uno studio restano nello studio.

> **Tre principi di prodotto.** Ogni dato dell'atto viene dai documenti, con la fonte, o è «N/D»: niente di inventato. L'avvocato rivede e decide; firma e deposito restano suoi. Ogni novità è un'opzione: spenta, il flusso resta identico a prima, e la scelta si congela sull'atto alla creazione.

02 COME LO PROTEGGIAMO

Dodici controlli in essere, ciascuno con la sua prova

Verificati sul codice in produzione e su AWS al 01/12/2026; le prove si mostrano in audit. Dettaglio nel documento 05 e nella dichiarazione di applicabilità (14).

IN ESSERE

Secondo fattore per tutti

Login Amazon Cognito solo su invito, app di autenticazione (TOTP) obbligatoria per ogni utente. MFA anche su ogni console amministrativa; credenziali amministrative solo temporanee (IAM Identity Center).

Pool Cognito: MFA «ON» · nessuna chiave statica

IN ESSERE

Token verificato a ogni richiesta

Firma, scadenza e destinatario del token controllati su ogni chiamata. Ruoli di studio (amministratore, membro, operatore, sola lettura) imposti dal server, non solo nascosti nell'interfaccia.

Verifica del token e ruoli coperti da test

IN ESSERE

Studi isolati tra loro

Ogni lettura dei dati di un cliente passa da un unico predicato di visibilità. Anche la cache del testo riconosciuto e del layout è dello studio, mai condivisa. Dentro lo studio ogni cliente ha la sua visibilità.

Predicato unico e test multi-tenant

IN ESSERE

Modelli solo nell'UE

Tutti gli agenti su Claude in Amazon Bedrock nella regione di Francoforte (UE), firmati dal ruolo dell'istanza; il codice rifiuta le regioni fuori dall'Unione. Embeddings Amazon Titan nell'UE. Opt-out dai servizi AI di AWS.

Configurazione Bedrock · policy di AWS Organizations

IN ESSERE

Cifratura ovunque

Dischi, copie e archivio temporaneo cifrati (AES-256, AWS KMS). TLS 1.2 o superiore, HSTS di un anno, intestazioni di sicurezza (CSP, frame-ancestors, Referrer-Policy). Password mai conservate da Trailgun.

Volume e copie cifrati in entrambe le regioni

IN ESSERE

Nessuna porta di amministrazione

In ingresso solo HTTPS. Nessun SSH: l'amministrazione passa da AWS Systems Manager, con sessioni registrate. IMDSv2 obbligatorio, container non root, proxy a versione fissata.

Infrastruttura descritta come codice (CDK)

IN ESSERE

Vedere e registrare

Accessi HTTP e log applicativi 90 giorni, mai testo dei documenti. CloudTrail su tutte le regioni con convalida d'integrità, 12 mesi; GuardDuty. Sonda esterna ogni minuto e allarmi 24/7.

Gruppi di log, trail, allarmi provati

IN ESSERE

Rilasci solo dopo i test

Controllo dei tipi, test unitari ed end-to-end obbligatori prima di ogni rilascio, anche manuale; branch di ambiente protetti. Scansione dei segreti su tutta la storia del codice, immagini e dipendenze analizzate.

CI con OIDC, gitleaks, ECR, Dependabot

IN ESSERE

Copie in due regioni, provate

Snapshot del disco dati ogni giorno alle 02:00 UTC e prima di ogni rilascio, conservati 14 giorni, copiati cifrati in Irlanda. Prova di ripristino automatica nella CI e trimestrale sullo snapshot reale, con RTO misurato.

Verbale della prova di ripristino

IN ESSERE

Regime per i fascicoli penali

Nessun indice di embeddings sui fascicoli penali o misti. Consultazioni (una all'ora per utente), domande, analisi e confronti fra depositi finiscono nel registro degli accessi dello studio.

Politica P16 · registro esportabile

IN ESSERE

IA dichiarata, sempre

I DOCX e i PDF generati dagli agenti portano nei metadati la marcatura «AI-generated, EU AI Act art. 50». Avviso di IA nelle chat, sulla pagina dell'atto e nelle mail inviate in modalità automatica.

Metadati XMP e IPTC · test dedicati

IN ESSERE

Fuori dalla piattaforma, niente pratiche

Notifiche via email, SMS, WhatsApp e Telegram senza dati delle pratiche. Ricerche su One LEGALE senza nomi, codici fiscali o importi. OCR di riserva fuori UE spento di default per ogni studio.

Regole in codice coperte da test

PERSONE E PROCESSI

security@ e privacy@trailgun.ai presidiate, reperibilità 24/7 per la priorità 1, DPO esterno nominato. Piano di continuità adottato; incidenti su tre livelli; registro delle violazioni. Fornitori valutati prima dell'ingaggio e ogni anno, con DPA firmati. Accessi del personale ai contenuti registrati; accessi privilegiati rivisti ogni trimestre. Formazione annuale; verifica dei precedenti per chi accede alla produzione; segreti dei fornitori ruotati ogni 12 mesi; polizze cyber e RC professionale.

03 DOVE VIVONO I DATI

A Francoforte, con le copie a Dublino. Anche i modelli.

Archivi, elaborazione e modelli di IA stanno nelle regioni AWS dell'Unione europea. Il produttore del modello non riceve i dati: il fornitore è AWS. Il documento 61 lo dichiara per iscritto.



CHE COSA	DOVE	PER QUANTO
Documenti, testi, elaborati, database	Disco cifrato a Francoforte	Finché lo studio non cancella la pratica o il cliente; a fine contratto al massimo 74 giorni (pagina «Impegni»)
Copie di sicurezza	Francoforte e Irlanda, cifrate	14 giorni, comprese le copie prima dei rilasci
File temporanei di OCR e audio	S3 a Francoforte, accesso pubblico bloccato	Cancellati a fine analisi, al massimo 1 giorno
Log di accesso e applicativi	CloudWatch a Francoforte	90 giorni, senza corpo delle richieste, token o testo dei documenti
Log di sicurezza e amministrazione	CloudTrail, sessioni SSM, accessi al backoffice	12 mesi, con convalida d'integrità
Testo inviato ai modelli	Amazon Bedrock, regione di Francoforte (UE)	Il tempo della richiesta; cache del prompt fino a 1 ora per l'analisi estesa del faldone
Email e notifiche	Resend su Amazon SES in Irlanda; Telegram, SMS e WhatsApp per chi li collega	Notifiche senza dati delle pratiche

L'elenco completo dei subfornitori, con entità, regione, meccanismo di trasferimento, certificazioni, DPA e sostituibilità, è nel Registro dei subfornitori (15) e su https://trailgun.ai/subprocessors. Microsoft non riceve dati da Trailgun: il file per la revisione in Word va dal browser al tenant dello studio.

04 IL CONFRONTO CHE CONTA

Come girano oggi i fascicoli, e come girano con Trailgun

Una banca, un servicer e uno studio si scambiano ogni giorno archivi di pratiche. Il rischio vero sta spesso nel tragitto: allegati, link, chiavette, cartelle condivise. Ecco la prassi più diffusa messa accanto a ciò che succede quando lo stesso archivio entra in Trailgun.

PRASSI DIFFUSA	CON TRAILGUN
Allegati via email Archivi di pratiche spediti come allegati, che restano in decine di caselle, sui telefoni e nei backup della posta di mittente e destinatari.	**Un archivio, un posto** L'archivio si carica una volta, su HTTPS, nello spazio dello studio: dal modulo, da una casella dedicata con mittenti verificati o via API con chiave dello studio.
Link di trasferimento senza password Chi ha il link scarica, senza autenticazione e spesso senza scadenza; nessuno sa chi l'ha aperto.	**Accesso solo con identità e secondo fattore** Login su invito, MFA obbligatoria per ogni utente, visibilità per cliente decisa dallo studio. Un'esportazione esce come archivio cifrato con link temporaneo.
Copie sparse Chiavette, cartelle condivise, PC personali: copie di cui nessuno tiene il conto e che nessuno cancella.	**Copie note, cancellazione verificabile** Le copie di sicurezza sono cifrate, in due regioni dell'Unione, conservate 14 giorni. Alla cancellazione di una pratica spariscono testi, indici, cache e conversazioni; a fine contratto arriva la conferma scritta.
Strumenti di IA generici Testi incollati in chat di uso generale, con server e condizioni d'uso che lo studio non controlla.	**Modelli nell'UE, nessun addestramento** Claude su Amazon Bedrock nella regione di Francoforte (UE), a condizioni che escludono l'addestramento e l'accesso del produttore del modello. Ogni file generato dichiara nei metadati che è generato con IA.
Nessuna traccia Chi ha letto il fascicolo, quando, che cosa ha cercato: di solito non si sa.	**Accessi registrati** Registro delle attività per studio; registro degli accessi ai fascicoli penali; accessi del personale di Trailgun ai contenuti solo su richiesta o per un incidente, registrati.
Fine del rapporto senza fine Quando l'incarico finisce, le copie restano dove sono arrivate: nessuno sa dirne il numero, nessuno ne certifica la cancellazione.	**Uscita con una data** 30 giorni di accesso in sola lettura con esportazione, cancellazione nei 30 successivi con certificato, copie fuori rotazione entro 14 giorni: al massimo 74 giorni dalla cessazione.

Che cosa resta allo studio. Decidere chi vede che cosa, rivedere ogni elaborato prima dell'uso, informare i propri clienti dell'uso dell'IA (il modello è il documento 19) e custodire le proprie credenziali. Trailgun dà gli strumenti: ruoli, visibilità per cliente, registro delle attività esportabile, cancellazione in ogni momento.

05 IMPEGNI

Gli stessi numeri in ogni documento

Livelli di servizio, ripristino, notifiche, conservazione: un'unica fonte per tutto il Pacchetto e per il contratto. Valgono dalla firma; dove una tappa del Percorso (12) li migliora, lo indica il suo codice.

IMPEGNO	VALORE	DOVE È SCRITTO
DISPONIBILITÀ		
Livello di servizio, 24 ore su 24	99,5 % mensile (99,9 % con la nuova piattaforma: Percorso, tappa R14)	55 · 01 All. A
Livello di servizio, giorni lavorativi 08:00-20:00	99,8 % mensile nella finestra, senza manutenzione programmata (99,95 %: tappa R14)	55
Misura	Sonda esterna ogni minuto su /api/health e sull'avvio di una lavorazione	55 · 05
Manutenzione programmata	Preavviso di almeno 48 ore; tra le 20:00 e le 07:00 o nel fine settimana; al massimo 8 ore al mese; una lavorazione interrotta si riavvia senza costi	55
Crediti di servizio	5 % da 99,0 % a meno di 99,5 %; 10 % da 98,0 %; 20 % da 97,0 %; sotto 97,0 % 30 % e diritto di recesso; tetto annuo 30 % dei corrispettivi	55
Rapporti sul servizio	Lavorazioni, atti e costi consultabili in app; rapporti mensili e trimestrali (tappa R04); questionari del cliente in 15 giorni lavorativi	55 · 18
ASSISTENZA · GIORNI LAVORATIVI 09:00-18:00, PRIORITÀ 1 ANCHE 24/7		
Priorità 1 · Bloccante	Presa in carico 1 ora, 24/7; soluzione o aggiramento 4 ore; aggiornamenti ogni 2 ore	55
Priorità 2 · Grave	Presa in carico 4 ore lavorative; soluzione o aggiramento 1 giorno lavorativo	55
Priorità 3 · Ordinaria e 4 · Richiesta	1 giorno lavorativo e 5 giorni lavorativi; 2 giorni lavorativi e pianificazione concordata	55
CONTINUITÀ E COPIE		
RPO, perdita massima di dati	24 ore (4 ore: tappa R01; 15 minuti: tappa R14)	55 · 11
RTO, guasto di istanza, disco o zona	8 ore di calendario dalla dichiarazione dell'incidente, misurato nelle prove trimestrali (4 ore: tappa R14)	55 · 11
Perdita della regione di Francoforte	Ripristino in Irlanda dalle copie che vi si trovano (RTO regionale: tappe R03 e R14)	11 · 31
Periodo massimo tollerabile di interruzione	5 giorni lavorativi; il deposito resta possibile con gli elaborati già scaricati	11
Copie di sicurezza	Ogni 24 ore e prima di ogni rilascio, in Germania e in Irlanda, cifrate, conservate 14 giorni	30 · P09
Prove di ripristino	Automatica a ogni verifica del codice; trimestrale sullo snapshot reale, in ambiente isolato, con verbale e misura dell'RTO; esito sempre ai clienti DORA	30 · 31

Esclusi dal calcolo della disponibilità la manutenzione programmata, la forza maggiore e i guasti del Cliente o dei servizi esterni che il Cliente sceglie (firma, visure, banche dati). Le date delle tappe sono solo nel documento 12, Percorso di certificazione e piattaforma.

05 IMPEGNI

Notifiche più strette dei termini del cliente

Il cliente DORA deve notificare un incidente grave entro 4 ore dalla classificazione e 24 dalla conoscenza: per questo la nostra prima notifica arriva entro 2 ore.

IMPEGNO	VALORE	DOVE È SCRITTO
INCIDENTI E VIOLAZIONI		
Incidente TIC: prima notifica	2 ore da quando Trailgun ne viene a conoscenza, per email e telefono; aggiornamenti almeno ogni 24 ore e a ogni cambiamento rilevante	18 · 25 · 51
Relazione intermedia e finale	48 ore dalla notifica iniziale, con i dati per i modelli del Reg. 2025/302; 20 giorni dalla chiusura	18 · 25
Minacce informatiche significative	Comunicazione entro 24 ore; assistenza negli incidenti senza costi aggiuntivi	18
Violazione di dati personali	Notifica al titolare entro 24 ore, per fasi se serve (art. 33 GDPR); registro delle violazioni con estratto al titolare	07 · 26
Richieste degli interessati, DPIA	Inoltro entro 3 giorni lavorativi; informazioni per la DPIA entro 10 giorni lavorativi	07 · 27 · 50
LOG E ACCESSI		
Accessi HTTP e log applicativi	90 giorni, mai corpo delle richieste, token o testo dei documenti	P08
Sicurezza e amministrazione	12 mesi: CloudTrail con convalida d'integrità, sessioni amministrative, accessi al backoffice	P08
Registro delle attività e accessi ai fascicoli penali	Per tutta la durata del contratto, consultabili ed esportabili dallo studio	P16
Accessi del personale	Ai contenuti solo su richiesta del cliente o per un incidente, registrati; revoca entro 24 ore; revisione trimestrale	22 · P03
FINE DEL CONTRATTO E USCITA		
Accesso dopo la cessazione	30 giorni in sola lettura con esportazione	07 · 56
Cancellazione	Entro i 30 giorni successivi, compresi testi, cache, conversazioni, indici e utenti; conferma scritta entro 5 giorni lavorativi; copie fuori rotazione entro 14 giorni: al massimo 74 giorni in tutto	28 · 54
Restituzione	Archivio ZIP cifrato: originali, elaborati DOCX e PDF/A, testi, dati in JSON e CSV, impronte SHA-256; entro 10 giorni lavorativi (in autonomia: tappa R02)	28 · 53 · 56
Assistenza all'uscita	30 giorni inclusi; fino a 12 mesi per i clienti DORA, con continuità del servizio	56 · 18
SUBFORNITORI, AUDIT, VULNERABILITÀ		
Cambio di subfornitore	Preavviso di 30 giorni, 60 per le funzioni essenziali o importanti; diritto di opposizione; urgenze comunicate entro 72 ore	07 · 15
Audit	Uno all'anno con 30 giorni di preavviso; illimitati per le funzioni essenziali o importanti DORA e per le autorità; questionari in 15 giorni lavorativi	18 · 52
Correzione delle vulnerabilità	Critica 72 ore; alta 7 giorni; media 30; bassa 90; aggiornamenti di sicurezza mensili del sistema operativo	24 · P07
Penetration test indipendente	Ogni anno e dopo ogni cambiamento rilevante; sintesi al cliente sotto riservatezza (tappa R06)	12

I termini di notifica sono impegni contrattuali di Trailgun, più stretti dei termini di legge del cliente per lasciargli margine (art. 19 DORA e Reg. del. (UE) 2025/301; art. 33 GDPR).

06 LE NORME

DORA, privacy e AI Act: che cosa vuol dire per voi

DORA · REG. (UE) 2022/2554

Il contratto vi dà tutto l'art. 30

- **Per gli intermediari 106** gli artt. 28 (salvo il par. 2), 29 e 30 si applicano **dal 1° gennaio 2027**, in regime semplificato (D.Lgs. 23/2025, artt. 6 e 17).
- **Tutte le clausole** dell'art. 30, par. 2, e, per le funzioni essenziali o importanti, del par. 3: livelli di servizio quantitativi, piani testati, TLPT, audit illimitati, uscita con periodo di transizione. Sono nell'Allegato DORA (18), con la mappa (17).
- **Funzione essenziale o importante**: la valuta il cliente. Trailgun offre a tutti le stesse clausole.
- **Subappalto** (Reg. del. 2025/532): 60 giorni di preavviso; il cambiamento non si attua prima della scadenza né con un'opposizione pendente.
- **Autorità**: Trailgun collabora con accessi, ispezioni e convocazioni presso di sé (art. 8 D.Lgs. 23/2025).
- **Registro delle informazioni**: tipo di servizio S19, catena dei subfornitori, dati per i modelli B_02, B_05, B_06, B_07 nella scheda 16; LEI [LEI].
- **Concentrazione**: AWS EMEA SARL è fornitore terzo critico designato il 18/11/2025; Trailgun no, ed è fuori dai criteri dell'art. 31.

GDPR · REG. (UE) 2016/679

Responsabile, con un DPA da firmare

- **Ruoli**: responsabile per i dati delle pratiche (art. 28); titolare autonomo solo per account, sicurezza, assistenza e fatturazione.
- **Dati giudiziari**: regime rafforzato per il penale (P16); DPO esterno nominato (art. 37, par. 1, lett. c).
- **Registro del responsabile** (art. 30, par. 2) nel foglio 40; supporto alla vostra DPIA nel documento 50.

AI ACT · REG. (UE) 2024/1689 E 2026/1744

Non ad alto rischio, trasparente

- **Classificazione**: l'Allegato III, punto 8(a), riguarda i sistemi usati da un'autorità giudiziaria o per suo conto; Trailgun non valuta il merito creditizio di persone fisiche (punto 5(b)). Questi usi sono esclusi dal contratto.
- **Art. 50**: avviso di IA nelle chat e nelle mail automatiche; marcatura leggibile da macchina in DOCX e PDF, in essere (art. 50, par. 2).
- **Art. 4**: formazione annuale del personale e sessione d'avvio per gli utenti. **L. 132/2025, art. 13**: modello di informativa ai clienti dello studio (19).
- **Modello**: Anthropic ha firmato il codice di buone pratiche per i modelli per finalità generali.

Il calendario che vi riguarda

DATA	CHE COSA SI APPLICA	CHE COSA FA TRAILGUN
17/01/2025	DORA per le entità finanziarie (art. 64)	Clausole dell'art. 30 nel contratto e nell'Allegato DORA (18)
02/08/2026	AI Act, applicazione generale, compreso l'art. 50	Avviso di IA nelle chat, sulla pagina dell'atto e nelle mail automatiche
02/12/2026	Marcatura dei contenuti generati per i sistemi già sul mercato (art. 50, par. 2, e art. 111, par. 4)	Metadati «AI-generated, EU AI Act art. 50» in DOCX e PDF, già in essere
01/01/2027	DORA per gli intermediari 106, in regime semplificato (D.Lgs. 23/2025, art. 17)	Stesse clausole e stessi tempi di notifica delle banche
12/01/2027	Data Act: nessun costo di passaggio ad altro fornitore (art. 29)	Esportazione in formati aperti, senza costi di uscita (56)
02/12/2027	AI Act: obblighi per l'alto rischio dell'Allegato III	Non applicabili nella finalità dichiarata; usi ad alto rischio esclusi dal contratto

NIS2. Trailgun non rientra nell'ambito del D.Lgs. 138/2024: un SaaS è un servizio di cloud computing, ma la soglia dimensionale si applica e Trailgun è sotto i massimali delle piccole imprese; la posizione completa è nel documento 62. **Data Act.** Passaggio ad altro fornitore con i dati in formati aperti (Reg. (UE) 2023/2854, art. 29).

07 VERIFICHE E CERTIFICAZIONI

Le prove si mostrano. Il percorso è scritto.

Trailgun lavora sulla norma ISO/IEC 27001 con una dichiarazione di applicabilità dei 93 controlli, diciassette politiche approvate e dodici procedure operative. La certificazione e le verifiche indipendenti hanno ciascuna la sua tappa nel documento 12.

STANDARD O VERIFICA	STATO	CHE COSA TROVATE NEL PACCHETTO
ISO/IEC 27001:2022	Sistema di gestione impostato sulla norma; certificato alla tappa R16 del Percorso	Dichiarazione di applicabilità dei 93 controlli dell'Allegato A, con stato ed evidenza (14); politiche P01-P17 (raccolte nel 10); procedure 20-31
Infrastruttura AWS	Ereditate: ISO/IEC 27001, 27017, 27018, SOC 2, C5	Rapporti da AWS Artifact su richiesta
Prove di ripristino	Automatica a ogni verifica del codice; trimestrale sullo snapshot reale, con RTO misurato	Verbale dell'ultima prova, su richiesta; sempre ai clienti DORA
Scansioni	Ogni immagine (ECR), dipendenze ogni settimana, segreti su tutta la storia del codice a ogni verifica	Tempi di correzione e segnalazione responsabile (24); https://trailgun.ai/security
Penetration test	Primo test indipendente alla tappa R06, poi ogni anno	Sintesi dei risultati e piano di rimedio, sotto riservatezza
ISO/IEC 42001 (IA)	Valutazione come obiettivo (tappa R17)	Governance dell'IA nel documento 09 e nella politica P15
Questionari del cliente	Risposta entro 15 giorni lavorativi, uno all'anno senza costi	Questionario precompilato (13); mappe EBA (48), GDPR (46) e AI Act (47)
Audit del cliente e delle autorità	Ordinario uno all'anno; illimitati per le funzioni essenziali o importanti DORA	Diritti di accesso, ispezione e copia nel documento 08 e nell'Allegato DORA (18); modulo di richiesta (52)

GLI ELEMENTI DI GARANZIA

L'RTS sulla politica dei fornitori ammette, accanto alle certificazioni, i vostri audit, i rapporti indipendenti, gli audit interni del fornitore e le informazioni che il fornitore dà (Reg. del. (UE) 2024/1773, art. 6, par. 3). Questo Pacchetto è la quarta voce: le evidenze dei registri 40-45 e della dichiarazione di applicabilità si mostrano in sede di audit.

INCIDENTI NEGLI ULTIMI 12 MESI

Uno: il 21/10/2026 un riavvio della produzione non è andato a buon fine per il disco di sistema pieno. Un incidente operativo di disponibilità, senza perdita né esposizione di dati, registrato nel registro degli incidenti con cause e azioni correttive, tra cui gli allarmi sullo spazio disco oggi attivi.

Perché lo diciamo così. L'RTS 2024/1773 chiede al cliente di non basarsi nel tempo solo su certificazioni e di verificarne perimetro, attualità e la prova dell'efficacia dei controlli. Preferiamo darvi elementi verificabili, farvi vedere le evidenze e scrivere le tappe con le loro date, piuttosto che un'etichetta. Trailgun non dichiara certificazioni proprie prima della tappa R16.

08 IL PACCHETTO DI CONFORMITÀ

Settanta documenti, ognuno per una domanda

48 PDF, 14 fogli di calcolo e 8 documenti Word. Chiedete quello che vi serve, quando vi serve: la colonna «Quando chiederlo» dice il momento in cui di solito lo si usa. Ogni documento cita gli altri con questo numero.

N.	DOCUMENTO	FORMATO	PER CHI	QUANDO CHIEDERLO
PANORAMICA E PERCORSO · 2				
00	Trust Center	PDF	Tutti: ufficio fornitori, ICT risk, DPO, soci dello studio	Sempre, per primo; da solo al primo contatto
12	Percorso di certificazione e piattaforma	PDF	ICT risk, vendor risk, audit	Con il 05 e il 08; a chi chiede certificazioni, pen test, escrow o alta disponibilità
CONTRATTO E ACCORDI DA FIRMARE · 8				
01	Contratto di servizio	PDF	Legale del cliente, ufficio acquisti	Alla negoziazione, da firmare
04	Accordo sul trattamento dei dati (DPA) per lo studio	PDF	Studi legali (titolari)	Alla firma con uno studio
07	Accordo sul trattamento dei dati (DPA)	PDF	Legale, DPO	Alla negoziazione del contratto, da firmare
18	Allegato DORA al contratto	Word	Legale del cliente	Alla negoziazione, con i clienti DORA
55	Accordo sul livello di servizio (SLA)	PDF	Legale, ufficio acquisti, ICT risk	Alla negoziazione, allegato al contratto
56	Piano di uscita e di transizione	PDF	Outsourcing, ICT risk, legale	Ai clienti DORA; con la strategia di uscita del cliente
57	Deposito del codice (escrow): term sheet	PDF	Legale, outsourcing	Ai clienti DORA con funzioni essenziali o importanti
58	Accordo sul trattamento dei dati (DPA), versione modificabile	Word	Legale e DPO del cliente	Quando il cliente vuole negoziare il DPA sul proprio testo
SICUREZZA, CONTINUITÀ E DORA · 4				
05	Sicurezza delle informazioni	PDF	Vendor risk, ICT risk, CISO del cliente	Con il questionario, all'avvio della valutazione del fornitore
08	DORA: Trailgun come fornitore di servizi TIC	PDF	ICT risk, outsourcing, compliance di banche, 106 e servicer	A ogni cliente DORA; prima del 1° gennaio 2027 a tutti i 106
10	Politiche di sicurezza e conformità (raccoglitore)	PDF	Audit, ICT risk	In sede di audit o quando il cliente chiede tutte le politiche insieme
11	Continuità operativa, ripristino e incidenti	PDF	ICT risk, BCM, DPO	Ai clienti DORA con funzioni essenziali o importanti; su richiesta
DATI PERSONALI E INTELLIGENZA ARTIFICIALE · 6				
02	Protezione dei dati (sintesi per lo studio)	PDF	Soci e DPO dello studio	Con il contratto, agli studi legali
03	AI e fiducia	PDF	Soci dello studio, compliance	Al primo incontro con uno studio
06	Protezione dei dati personali	PDF	DPO, ufficio privacy, studi	Con il DPA; quando il cliente prepara la DPIA
09	AI Act e uso dell'IA nella professione	PDF	Compliance, DPO, studi	Con il 06; a ogni studio legale
19	Informativa sull'IA ai clienti dello studio	Word	Studi	All'avvio di uno studio
50	Supporto alla valutazione d'impatto (DPIA) del Titolare	Word	DPO del cliente	Quando il cliente prepara la DPIA
DICHIARAZIONI · 3				
60	Dichiarazione: nessun addestramento sui dati dei clienti	PDF	Compliance, DPO, soci dello studio	Sempre con il 00 agli studi; su richiesta
61	Dichiarazione: localizzazione dei dati nell'Unione europea	PDF	DPO, ICT risk	Sempre con il 00 alle banche; su richiesta
62	Posizione di Trailgun rispetto alla NIS2	PDF	Compliance di clienti soggetti NIS2, ICT risk	Su richiesta

N.	DOCUMENTO	FORMATO	PER CHI	QUANDO CHIEDERLO
POLITICHE · 17				
P01	Politica di sicurezza delle informazioni	PDF	Audit, ICT risk	Su richiesta della politica di sicurezza
P02	Politica di gestione del rischio ICT	PDF	ICT risk, audit	Ai clienti DORA; in audit
P03	Politica di controllo degli accessi	PDF	ICT risk, audit	Su richiesta
P04	Politica di crittografia e gestione delle chiavi	PDF	ICT risk, CISO	Su richiesta
P05	Politica di sicurezza delle operazioni e gestione dei cambiamenti	PDF	ICT risk, audit	Su richiesta
P06	Politica di sviluppo sicuro	PDF	ICT risk, CISO	Su richiesta
P07	Politica di gestione delle vulnerabilità	PDF	ICT risk, CISO	Su richiesta
P08	Politica di logging e monitoraggio	PDF	ICT risk, audit	Su richiesta
P09	Politica di backup e ripristino	PDF	ICT risk, BCM	Su richiesta
P10	Politica di gestione dei fornitori ICT	PDF	Outsourcing, ICT risk	Ai clienti DORA
P11	Politica di classificazione e trattamento delle informazioni	PDF	Audit, DPO	Su richiesta
P12	Politica di conservazione e cancellazione	PDF	DPO, audit	Con il DPA, su richiesta
P13	Politica di sicurezza del personale e formazione	PDF	Audit, HR del cliente	Su richiesta
P14	Politica di uso accettabile	PDF	Audit	Su richiesta
P15	Politica di governance dell'intelligenza artificiale	PDF	Compliance, DPO, studi	Con il 09
P16	Politica sui fascicoli penali: regime rafforzato	PDF	Studi penalisti, DPO	A ogni studio che tratta fascicoli penali
P17	Politica di gestione delle segnalazioni (whistleblowing)	PDF	Compliance	Su richiesta
PROCEDURE · 12				
20	Procedura di gestione dei cambiamenti	PDF	ICT risk, audit	In audit; su richiesta
21	Procedura di ingresso e uscita del personale	PDF	Audit, HR del cliente	In audit
22	Procedura di revisione degli accessi	PDF	ICT risk, audit	In audit
23	Procedura di gestione delle chiavi e dei segreti	PDF	ICT risk, CISO	Su richiesta
24	Procedura di gestione delle vulnerabilità e di segnalazione responsabile	PDF	CISO, ricercatori di sicurezza	Su richiesta; è anche il testo pubblico di https://trailgun.ai/security
25	Procedura di risposta agli incidenti (runbook)	PDF	ICT risk, SOC del cliente	Ai clienti DORA; in audit
26	Procedura per le violazioni dei dati personali	PDF	DPO	Con il DPA
27	Procedura per le richieste degli interessati	PDF	DPO	Con il DPA
28	Procedura di restituzione e cancellazione a fine contratto	PDF	DPO, legale, outsourcing	Con il DPA e il piano di uscita (56)
29	Procedura di valutazione dei fornitori	PDF	Outsourcing, DPO	Ai clienti DORA; con il registro 15
30	Procedura di backup e ripristino (runbook)	PDF	ICT risk, BCM	Ai clienti DORA; in audit
31	Programma di prova di disaster recovery	PDF	ICT risk, BCM, audit	Ai clienti DORA con funzioni essenziali o importanti
FOGLI DI CALCOLO: QUESTIONARIO, REGISTRI E MAPPE · 14				
13	Questionario fornitore precompilato	Excel	Vendor risk	Con il 05, o per compilare il questionario del cliente
14	Dichiarazione di applicabilità ISO/IEC 27001	Excel	ICT risk, auditor	Quando il cliente chiede la SoA o il percorso ISO
15	Registro dei subfornitori	Excel	DPO, ICT risk, outsourcing	Con il DPA (è l'elenco dei sub-responsabili) e con il 08
16	Scheda per il Registro delle informazioni	Excel	Chi tiene il registro DORA del cliente	Alla firma, ai clienti DORA

N.	DOCUMENTO	FORMATO	PER CHI	QUANDO CHIEDERLO
17	Mappa DORA	Excel	ICT risk, legale	Con il 08
40	Registro dei trattamenti del responsabile (art. 30, par. 2, GDPR)	Excel	DPO	Con il DPA; su richiesta del Garante o del Titolare
41	Registro dei rischi ICT	Excel	ICT risk, audit	Ai clienti DORA; in audit
42	Inventario degli asset	Excel	ICT risk, audit	In audit; ai clienti DORA che lo chiedono
43	Registro della formazione (modello)	Excel	Audit	In audit
44	Revisione degli accessi (modello)	Excel	Audit, ICT risk	In audit
45	Registro dei cambiamenti (modello)	Excel	Audit	In audit
46	Mappa GDPR art. 28, par. 3 → DPA	Excel	DPO, legale	Con il DPA
47	Mappa AI Act → controlli	Excel	Compliance, DPO	Con il 09
48	Mappa linee guida EBA sull'esternalizzazione → clausole	Excel	Outsourcing di banche e 106	A chi valuta il fornitore con lo schema EBA o la Circolare 288
MODELLI E CERTIFICATI · 4				
51	Modelli di notifica degli incidenti (iniziale, intermedia, finale, minaccia)	Word	ICT risk e funzione incidenti del cliente	Ai clienti DORA, alla firma
52	Modulo di richiesta di audit	Word	Audit interno del cliente, autorità	Su richiesta di un audit
53	Certificato di restituzione dei dati	Word	Titolare, DPO	All'esportazione finale
54	Certificato di cancellazione	Word	Titolare, DPO	Entro 5 giorni lavorativi dalla cancellazione

PACCHETTI PRONTI

Che cosa inviamo, a chi

Per non farvi chiedere documento per documento, li raggruppiamo così. Ogni pacchetto si integra su richiesta con qualunque altro documento dell'indice.

PACCHETTO	DOCUMENTI
Primo contatto	00 Trust Center · 60 Dichiarazione: nessun addestramento sui dati dei clienti · 61 Dichiarazione: localizzazione dei dati nell'Unione europea
Banca, 106 o servicer: valutazione del fornitore	00 Trust Center · 05 Sicurezza delle informazioni · 08 DORA: Trailgun come fornitore di servizi TIC · 12 Percorso di certificazione e piattaforma · 13 Questionario fornitore precompilato · 15 Registro dei subfornitori · 17 Mappa DORA · 48 Mappa linee guida EBA sull'esternalizzazione → clausole · 60 Dichiarazione: nessun addestramento sui dati dei clienti · 61 Dichiarazione: localizzazione dei dati nell'Unione europea
Contratto con un cliente DORA	01 Contratto di servizio · 07 Accordo sul trattamento dei dati (DPA) · 18 Allegato DORA al contratto · 55 Accordo sul livello di servizio (SLA) · 56 Piano di uscita e di transizione · 57 Deposito del codice (escrow): term sheet · 16 Scheda per il Registro delle informazioni · 51 Modelli di notifica degli incidenti (iniziale, intermedia, finale, minaccia) · 11 Continuità operativa, ripristino e incidenti
DPO del cliente	06 Protezione dei dati personali · 07 Accordo sul trattamento dei dati (DPA) · 09 AI Act e uso dell'IA nella professione · 15 Registro dei subfornitori · 40 Registro dei trattamenti del responsabile (art. 30, par. 2, GDPR) · 46 Mappa GDPR art. 28, par. 3 → DPA · 50 Supporto alla valutazione d'impatto (DPIA) del Titolare · 26 Procedura per le violazioni dei dati personali · 27 Procedura per le richieste degli interessati · 28 Procedura di restituzione e cancellazione a fine contratto
Studio legale	00 Trust Center · 01 Contratto di servizio · 02 Protezione dei dati (sintesi per lo studio) · 03 AI e fiducia · 04 Accordo sul trattamento dei dati (DPA) per lo studio · 09 AI Act e uso dell'IA nella professione · 19 Informativa sull'IA ai clienti dello studio · 60 Dichiarazione: nessun addestramento sui dati dei clienti · P16 Politica sui fascicoli penali: regime rafforzato
Audit	Tutti i 70 documenti, più le evidenze indicate nella dichiarazione di applicabilità 14 e nei registri 40-45 (si mostrano, non si consegnano)

09 CONTATTI

Una persona risponde, a ogni ora per la priorità 1

Le segnalazioni di sicurezza e gli incidenti vanno a security@; le domande sui dati personali, le richieste degli interessati e il DPO a privacy@. Le vulnerabilità si segnalano come da https://trailgun.ai/security e /.well-known/security.txt.

SICUREZZA E INCIDENTI
security@trailgun.ai
presidiata 24/7 per la priorità 1; risposta automatica con il numero di reperibilità

PRIVACY
privacy@trailgun.ai
richieste del Titolare, degli interessati e del DPO

DPO
[DPO esterno: nome o società]
[dpo@...]

REPERIBILITÀ PRIORITÀ 1
[+39 ...]
24 ore su 24, solo priorità 1

ASSISTENZA
In app e info@trailgun.ai
cuffie nella barra in alto: agente e ticket; giorni lavorativi 09:00-18:00

REFERENTE CONTRATTUALE
Franco Puppo, CEO
legale rappresentante e responsabile della sicurezza; [email]

SOCIETÀ	DATI
Ragione sociale	[Trailgun S.r.l.]
Sede legale	[indirizzo]
P.IVA e C.F.	[...]
Registro delle imprese e REA	[...]
PEC	[...]
LEI	[...]
Legale rappresentante	Franco Puppo, CEO
Cofondatore	Alessandro Musella, avvocato: metodo e legal design
Sito e piattaforma	https://trailgun.ai · https://app.trailgun.ai
Subfornitori	https://trailgun.ai/subprocessors

Riservatezza. Il Pacchetto è riservato al destinatario e serve alla valutazione di Trailgun come fornitore. I documenti contrattuali (01, 04, 07, 18, 55-58) diventano vincolanti solo con la firma. Questa è la versione 2.0, con lo stato al 01/12/2026; la prossima si emette a ogni tappa del Percorso o cambiamento rilevante.