Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO P01



VERSIONE 2.0 · DICEMBRE 2026

Politica di sicurezza delle informazioni

Come Trailgun protegge la disponibilità, l'autenticità, l'integrità e la riservatezza del servizio e dei dati che studi legali, banche e servicer le affidano. È la politica da cui discendono le altre sedici, le procedure 20-31 e i registri 40-45.

CODICE	TITOLARE	REVISIONE	STATO
P01 · POL-01	Responsabile della sicurezza	Annuale	al 01/12/2026

POLITICA P01 · POL-01

Politica di sicurezza delle informazioni

La politica quadro: principi, organizzazione, obiettivi e regole comuni a tutte le altre politiche di Trailgun.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P01 (POL-01)	Responsabile della sicurezza	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale; dopo ogni incidente grave e cambiamento rilevante	tutto il personale e i collaboratori; organo amministrativo; Clienti e loro autorità	Riservato · per il Cliente

DOCUMENTI COLLEGATI

P02–P17; documento 05 (Sicurezza delle informazioni); 11 (Continuità operativa, ripristino e incidenti); 12 (Percorso di certificazione e piattaforma); procedure 20–31; registri 40–45

AMBITO

La piattaforma Trailgun (app.trailgun.ai, backoffice.trailgun.ai, il sito trailgun.ai e l'API pubblica `/api/v1`) nei suoi tre ambienti (development, staging, production), i dati che tratta, le persone che vi lavorano a qualsiasi titolo e i fornitori che concorrono al servizio.

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
5.1–5.4, 5.31, 5.35–5.37; clausole 5–10	DORA artt. 5, 6, 9(4)(a), 30; GDPR artt. 24, 32

1 Scopo

Trailgun tratta per conto di studi legali, banche e servicer documenti coperti dal segreto professionale e dal segreto bancario, compresi atti di procedimenti penali. Questa politica fissa il modo in cui Trailgun protegge la disponibilità, l'autenticità, l'integrità e la riservatezza di quei dati e del servizio, nei termini dell'art. 9 del Regolamento (UE) 2022/2554 («DORA») e dell'art. 32 del Regolamento (UE) 2016/679 («GDPR»).

Trailgun è un fornitore terzo di servizi TIC (art. 3, punto 19, DORA): gli obblighi di DORA ricadono sui Clienti che sono entità finanziarie, e Trailgun li rende possibili con queste politiche, con le procedure che le attuano e con il contratto (art. 30 DORA; documento 18, Allegato DORA al contratto).

2 Principi

2.1 **Verità.** Nessun documento di Trailgun dichiara un controllo che non esiste. Ogni affermazione sulla piattaforma rimanda a un'evidenza nel codice, sull'infrastruttura o in un registro. Ciò che è in programma sta in un solo posto, il documento 12 (Percorso di certificazione e piattaforma), con la sua data.

2.2 **Necessità e minimo privilegio.** Persone, servizi e fornitori accedono solo ai dati e ai sistemi che servono al loro compito, e solo per il tempo necessario (politica P03).

2.3 **Dati nell'Unione europea.** I dati dei Clienti si conservano e si elaborano nell'Unione europea: l'infrastruttura è su Amazon Web Services a Francoforte (eu-central-1), con le copie di sicurezza in Irlanda (eu-west-1); i modelli di linguaggio e gli embeddings girano su Amazon Bedrock in una regione dell'UE e il codice rifiuta qualsiasi regione fuori dall'UE. I pochi fornitori con sede fuori dall'UE trattano nell'UE o con garanzie adeguate e sono elencati, con le garanzie, nella politica P10 e nel registro 15.

2.4 **Nessun addestramento.** I dati dei Clienti non addestrano modelli, né di Trailgun né dei fornitori dei modelli (politica P15).

2.5 **Sicurezza fin dalla progettazione.** Ogni funzione nuova nasce come opzione attivabile e disattivabile; spenta, il flusso resta identico a prima. Ogni dato di un elaborato viene dai documenti, con la fonte, o è dichiarato «N/D».

2.6 **Difesa in profondità.** Nessun controllo è l'unica barriera per i dati di un Cliente: autenticazione forte, visibilità applicativa, rete, cifratura, registri e copie si sommano.

2.7 **Separazione fra studi.** I dati di uno studio non sono mai visibili a un altro. Ogni interrogazione su dati di un cliente passa da un unico predicato di visibilità, coperto da test automatici.

3 Obiettivi misurabili

Gli obiettivi di sicurezza coincidono con gli impegni verso i Clienti e sono identici in tutti i documenti del pacchetto:

- disponibilità mensile del 99,5% (99,8% nella finestra dei giorni lavorativi 08:00-20:00), misurata ogni minuto da una sonda esterna;
- RPO di 24 ore, RTO di 8 ore nella stessa regione, periodo massimo tollerabile di interruzione di 5 giorni lavorativi;
- notifica iniziale di un incidente TIC al Cliente entro 2 ore dalla conoscenza; notifica di una violazione dei dati personali al Titolare entro 24 ore;
- correzione delle vulnerabilità critiche entro 72 ore, alte entro 7 giorni, medie entro 30, basse entro 90.

Il Responsabile della sicurezza li misura, li riporta all'organo amministrativo nella relazione annuale e li comunica al Cliente che lo chiede, sempre ai Clienti DORA. Il rapporto di servizio periodico e i livelli di servizio della nuova piattaforma sono le tappe R04, R01 e R14 del Percorso (documento 12).

4 Organizzazione e responsabilità

4.1 **Organo amministrativo.** Approva le politiche, la propensione al rischio e i piani di trattamento dei rischi alti e critici; riceve almeno una volta all'anno la relazione del Responsabile della sicurezza sullo stato dei controlli, degli incidenti, delle prove e dei fornitori, e ne verbalizza l'esame.

4.2 **Responsabile della sicurezza.** Franco Puppo, CEO e legale rappresentante. Attua le politiche, tiene i registri, guida la risposta agli incidenti ed è il referente dei Clienti e delle autorità per la sicurezza. La nomina di un responsabile dedicato è la tappa R13 del Percorso.

4.3 **Responsabile della protezione dei dati (DPO).** Esterno, [DPO esterno: nome o società], designato ai sensi dell'art. 37, par. 1, lett. c), GDPR, perché il trattamento di dati relativi a reati per conto degli studi è un'attività principale di Trailgun, e comunicato al Garante (art. 37, par. 7). Sorveglia le politiche P10, P11, P12 e P16 e la gestione delle violazioni. Contatti: [dpo@...] e privacy@trailgun.ai.

4.4 **Responsabile della conformità IA.** [nome], titolare della politica P15. Alessandro Musella, cofondatore e avvocato, contribuisce al metodo giuridico e al legal design dei flussi, senza ruoli esecutivi né accessi alla produzione.

4.5 **Separazione dei compiti.** In una squadra tecnica piccola la separazione dei compiti si ottiene con controlli che nessuno può saltare: branch di ambiente protetti, con pull request e verifica automatica obbligatoria (anche per il rilascio di production lanciato a mano); credenziali amministrative solo temporanee; registri di amministrazione a prova di manomissione per 12 mesi; sessioni sulla macchina registrate; registro degli accessi del personale al contenuto; revisione trimestrale degli accessi privilegiati; diritti di audit dei Clienti. Il penetration test indipendente e il responsabile della sicurezza dedicato sono le tappe R06 e R13.

4.6 **Personale e collaboratori.** Conoscono le politiche che li riguardano, le rispettano e segnalano subito a security@trailgun.ai ogni evento di sicurezza osservato o sospetto.

5 Quadro documentale e registri

Le politiche P02-P17 attuano questa politica; le procedure 20-31 ne sono i passi operativi e il documento 11 è il piano di continuità e di gestione degli incidenti. Trailgun tiene questi registri, ognuno con chi l'ha aggiornato e quando:

- trattamenti svolti come responsabile (40); rischi ICT (41); asset (42); formazione (43); revisioni degli accessi (44); cambiamenti (45);
- incidenti e minacce significative (procedura 25); violazioni dei dati personali (procedura 26); fornitori e loro valutazioni (registro 15, procedura 29);
- accessi del personale al contenuto delle pratiche (politica P03); eccezioni (§ 8); verbali delle prove di ripristino (procedure 30 e 31).

6 Conformità alle norme

6.1 Trailgun individua le norme applicabili e le riesamina ogni anno: DORA e i suoi atti di livello 2 per i Clienti finanziari; il D.Lgs. 10 marzo 2025, n. 23, che applica agli intermediari ex art. 106 TUB gli artt. 28 (salvo il par. 2), 29 e 30, par. 1-4, DORA (art. 6) dal 01/01/2027 (art. 17); GDPR e Codice privacy; il Regolamento (UE) 2024/1689 («AI Act») come modificato dal Regolamento (UE) 2026/1744; la L. 23 settembre 2025, n. 132; il Regolamento (UE) 2023/2854 («Data Act»).

6.2 Trailgun coopera pienamente con le autorità competenti dei Clienti e con le persone da esse incaricate (art. 30, par. 2, lett. g), DORA), anche negli accessi e nelle ispezioni presso i fornitori previsti dall'art. 8 del D.Lgs. 23/2025. La mancata collaborazione è sanzionata anche in capo al fornitore (art. 144, c. 8-bis, TUB).

6.3 Trailgun non è un fornitore terzo critico designato (art. 31 DORA) e non rientra nell'ambito del D.Lgs. 4 settembre 2024, n. 138 (NIS2), perché sotto la soglia della media impresa (documento 62, Posizione di Trailgun rispetto alla NIS2). La valutazione si ripete ogni anno e a ogni variazione di addetti o fatturato.

7 Verifica e miglioramento

L'efficacia dei controlli si verifica con continuità e a scadenza fissa:

- a ogni cambiamento: la verifica automatica della CI (controllo dei tipi, test unitari ed end-to-end, scansione dei segreti su tutta la storia del repository, prova di ripristino del database);
- ogni trimestre: la prova di ripristino sullo snapshot reale con l'RTO misurato e il verbale; la revisione degli accessi privilegiati; il riesame dei trattamenti del registro dei rischi;
- ogni anno: la valutazione dei fornitori, il riesame delle politiche, la relazione all'organo amministrativo; in ogni momento, gli audit dei Clienti e delle loro autorità.

Le verifiche esterne e la certificazione seguono il Percorso: scansione esterna dell'applicazione (R05), penetration test indipendente (R06), gap assessment, sistema di gestione, audit di stage 1 e certificato ISO/IEC 27001:2022 (R07, R08, R15, R16). Ogni non conformità diventa una voce del registro dei rischi (41) con un titolare e una data.

8 Eccezioni (regola comune a tutte le politiche)

8.1 Un'eccezione a una politica si chiede per iscritto al Responsabile della sicurezza, con il motivo, i dati e i sistemi coinvolti, le misure compensative e la durata.

8.2 Il Responsabile della sicurezza valuta il rischio con il metodo della politica P02. Un'eccezione che lascia un rischio alto o critico la approva l'organo amministrativo.

8.3 Ogni eccezione si annota nel registro delle eccezioni, con una scadenza non successiva alla revisione annuale seguente, e si chiude o si rinnova motivando. Un'eccezione che riguarda i dati di un Cliente DORA che usa Trailgun per una funzione essenziale o importante gli si comunica.

8.4 Nessuna eccezione è silenziosa: un controllo che non si applica è una voce del registro dei rischi, con il trattamento e il titolare.

9 Violazioni delle politiche

La violazione di una politica da parte del personale si valuta secondo il contratto di lavoro o di collaborazione e la legge applicabile; da parte di un fornitore, secondo il contratto con lui, fino alla risoluzione. Le violazioni che sono anche incidenti seguono la procedura 25 (Risposta agli incidenti).

10 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
Politiche approvate	IN ESSERE P01–P17, versione 2.0, approvate dall'organo amministrativo	verbale del [data]; riesame annuale
Ruoli nominati	IN ESSERE Responsabile della sicurezza; DPO esterno comunicato al Garante; responsabile della conformità IA	lettere di nomina; ricevuta del Garante
Contatti presidiati	IN ESSERE security@trailgun.ai e privacy@trailgun.ai; priorità 1 anche 24/7 al numero [+39 …]	risposta automatica con il numero di reperibilità
Registri	IN ESSERE 40–45 e i registri delle procedure 25, 26, 29, 30 e 31	aggiornati a ogni evento, riesaminati ogni trimestre
Relazione annuale	IN ESSERE stato dei controlli, incidenti, prove, fornitori, eccezioni	all'organo amministrativo, ogni anno
Certificazioni	quelle dell'infrastruttura AWS (ISO/IEC 27001, 27017, 27018, SOC 2, C5); il percorso di Trailgun verso la ISO/IEC 27001 è nel documento 12	rapporti da AWS Artifact, su richiesta

11 Riferimenti normativi

DORA artt. 5, 6, 9 e 30; Reg. del. (UE) 2024/1774 (titolo III per il quadro semplificato degli intermediari 106); D.Lgs. 23/2025 artt. 6, 8 e 17; art. 144, c. 8-bis, TUB; GDPR artt. 24, 25, 28, 32 e 37; ISO/IEC 27001:2022, clausole 5-10 e Allegato A, controlli 5.1-5.4, 5.31, 5.35-5.37.