Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO 10

VERSIONE 2.0 · DICEMBRE 2026

Politiche di sicurezza e conformità

Il corpo delle politiche di Trailgun in un solo volume: sicurezza delle informazioni, rischio ICT, accessi, crittografia, operazioni, sviluppo, vulnerabilità, log, backup, fornitori, classificazione, conservazione, personale, uso accettabile, intelligenza artificiale, fascicoli penali, segnalazioni. Con il registro dei rischi in sintesi e la mappa delle corrispondenze normative.

STATO	APPROVAZIONE	REVISIONE	CLASSIFICAZIONE
al 01/12/2026	Organo amministrativo	Annuale	Riservato · per il Cliente

COME SI LEGGE

Ogni regola, con la sua evidenza

Una politica dice che cosa deve accadere, chi ne risponde e come lo si dimostra. Ognuna delle diciassette chiude con le evidenze e i registri che la provano e rimanda alle procedure 20-31 per i passi operativi. Lo stato descritto è quello della piattaforma al 01/12/2026; ciò che è in programma sta solo nel documento 12, Percorso di certificazione e piattaforma, ed è richiamato qui con il codice della tappa (R01-R17).

CHI APPROVA

Organo amministrativo

Ha approvato le diciassette politiche, versione 2.0, il [data della delibera] e ne ha la responsabilità ultima. Le riesamina ogni anno con la relazione del Responsabile della sicurezza.

CHI LE APPLICA

Responsabile della sicurezza

Franco Puppo, CEO e legale rappresentante. È titolare o contitolare di quattordici politiche su diciassette, tiene i registri e guida la risposta agli incidenti.

CHI CONTROLLA

DPO e conformità IA

DPO esterno: [nome o società], comunicato al Garante. Responsabile della conformità IA: [nome]. I Clienti e le loro autorità hanno diritti di audit e di accesso (documento 18).

Le politiche

P01	Sicurezza delle informazioni	P02	Gestione del rischio ICT
P03	Controllo degli accessi	P04	Crittografia e gestione delle chiavi
P05	Operazioni e cambiamenti	P06	Sviluppo sicuro
P07	Gestione delle vulnerabilità	P08	Logging e monitoraggio
P09	Backup e ripristino	P10	Gestione dei fornitori ICT
P11	Classificazione delle informazioni	P12	Conservazione e cancellazione
P13	Personale e formazione	P14	Uso accettabile
P15	Governance dell'intelligenza artificiale	P16	Fascicoli penali
P17	Gestione delle segnalazioni	A·B	Registro dei rischi in sintesi · Mappa delle corrispondenze

Che cosa non è. Non è una certificazione: Trailgun non ne dichiara di proprie e il suo percorso verso la ISO/IEC 27001:2022 è nel documento 12. Ogni politica esiste anche come documento a sé (P01-P17), con lo stesso testo. Il registro dei rischi completo è il foglio 41; il piano di continuità e di gestione degli incidenti è il documento 11.

SUMMARY IN ENGLISH

Seventeen policies, approved and applied

This binder contains Trailgun's seventeen information security and compliance policies (P01–P17), each also issued as a separate document. It is written for the vendor-risk, ICT-risk and DPO offices of banks, NPL servicers (Italian financial intermediaries under art. 106 of the Banking Act, to which DORA arts. 28 (except para. 2), 29 and 30(1)-(4) apply from 1 January 2027 under arts. 6 and 17 of Legislative Decree 23/2025) and law firms. The full text is in Italian.

How each policy is built

Code, owner, approval by the board of directors, version 2.0 of 1 December 2026, annual review, audience, related documents, scope, ISO/IEC 27001:2022 Annex A controls and legal sources (DORA, Delegated Regulation (EU) 2024/1774, GDPR, AI Act); then purpose, roles, rules, numbered steps, the evidence and registers that prove the policy, exceptions and references. Operational steps are in procedures 20–31; the full ICT risk register is spreadsheet 41.

The platform on 1 December 2026

AWS in eu-central-1 (Frankfurt) with encrypted volumes and daily snapshots copied, encrypted, to eu-west-1 (Ireland). All agents run on Claude in Amazon Bedrock in an EU region and embeddings on Amazon Titan Text Embeddings V2 in the EU: the code refuses any non-EU region, and customer data trains no model. Amazon Cognito with mandatory TOTP for every user; temporary administrative credentials through IAM Identity Center and MFA on every console; CloudTrail in all regions with integrity validation for 12 months, GuardDuty and recorded SSM sessions; HTTP and application logs for 90 days, never with document text. An external probe every minute and 24/7 alarms. Protected environment branches and a mandatory CI check (type checks, unit and end-to-end tests, gitleaks secret scanning, database restore drill), enforced also on manual production releases; a quarterly restore drill on the real production snapshot with measured RTO. AI Act art. 50: machine-readable marking of generated DOCX and PDF files and AI notices in chats and automatic emails.

Key commitments (same figures in every document)

TOPIC	COMMITMENT
Availability	99.5% monthly 24/7; 99.8% in business hours (08:00–20:00), measured every minute
Recovery	RPO 24 h; RTO 8 h in the same region; maximum tolerable disruption 5 business days
ICT incidents	Initial notice 2 h, updates every 24 h, intermediate report 48 h, final report 20 days after closure; significant threats 24 h
Personal data breaches	Notice to the controller within 24 h
Vulnerabilities	Critical 72 h, high 7 days, medium 30 days, low 90 days; host OS image updated monthly
Access	MFA everywhere; quarterly privileged-access reviews; revocation within 24 h of departure
Exit	30 days read-only with export; full export within 10 business days; deletion within the following 30 days with written confirmation; backups expire within 14 days: 74 days at most

ISO/IEC 27001 certification, independent penetration testing, source-code escrow and the multi-AZ platform are dated milestones R01–R17 in document 12, «Certification and platform roadmap». Trailgun claims no certification of its own; AWS certifications are available through AWS Artifact.

QUADRO DELLE POLITICHE

Titolari, approvazione e cicli di revisione

Tutte le politiche sono alla versione 2.0 del 01/12/2026, approvate dall'organo amministrativo il [data della delibera] e riesaminate almeno una volta all'anno, dopo ogni incidente grave e a ogni cambiamento rilevante dell'architettura, dei fornitori o delle norme. La tabella riprende i dati di testa di ciascuna politica.

N.	POLITICA	TITOLARE	REVISIONE	ISO 27001 ALL. A	NORME PRINCIPALI
P01	**Sicurezza delle informazioni**	Responsabile della sicurezza	annuale; dopo ogni incidente grave e cambiamento rilevante	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
P02	**Gestione del rischio ICT**	Responsabile della sicurezza	metodo annuale; registro ogni trimestre e a ogni evento rilevante	5.7, 5.9; clausole 6.1, 8.2, 8.3	DORA artt. 6, 8, 16, 28(4), 29; Reg. del. (UE) 2024/1774
P03	**Controllo degli accessi**	Responsabile della sicurezza	annuale; accessi privilegiati ogni trimestre	5.15-5.18, 7.2, 8.2-8.5	DORA art. 9(4)(c)-(d); Reg. del. (UE) 2024/1774 artt. 19-21; GDPR art. 32
P04	**Crittografia e gestione delle chiavi**	Responsabile della sicurezza	annuale e a ogni cambio di algoritmo o servizio	8.24, 5.17, 8.20, 8.21	DORA art. 9(4)(d); Reg. del. (UE) 2024/1774 art. 6; GDPR art. 32(1)(a)
P05	**Operazioni e cambiamenti**	Responsabile della sicurezza	annuale	5.37, 8.6, 8.7, 8.9, 8.19, 8.31, 8.32	DORA art. 9(4)(e); Reg. del. (UE) 2024/1774
P06	**Sviluppo sicuro**	Responsabile della sicurezza	annuale	8.4, 8.25-8.30, 8.33	Reg. del. (UE) 2024/1774 art. 16; DORA art. 25; GDPR art. 25
P07	**Gestione delle vulnerabilità**	Responsabile della sicurezza	annuale	8.8, 5.7, 6.8	DORA artt. 9(4)(f), 25; Reg. del. (UE) 2024/1774 art. 10
P08	**Logging e monitoraggio**	Responsabile della sicurezza	annuale	8.15, 8.16, 8.17	DORA art. 10; Reg. del. (UE) 2024/1774 art. 12; GDPR art. 32
P09	**Backup e ripristino**	Responsabile della sicurezza	annuale e dopo ogni prova di ripristino	8.13, 8.14, 5.30	DORA artt. 11, 12; GDPR art. 32(1)(c)
P10	**Gestione dei fornitori ICT**	Responsabile della sicurezza, con il DPO	annuale; registro a ogni cambio di fornitore	5.19-5.23	DORA artt. 28-30; Reg. del. (UE) 2025/532; GDPR artt. 28, 44-46
P11	**Classificazione delle informazioni**	Responsabile della sicurezza, con il DPO	annuale	5.12-5.14, 8.11, 8.12	DORA art. 8; Reg. es. (UE) 2024/2956; GDPR artt. 9, 10, 32
P12	**Conservazione e cancellazione**	DPO e Responsabile della sicurezza	annuale	5.33, 8.10	GDPR artt. 5(1)(e), 28(3)(g); DORA art. 30(2)(d); Data Act art. 25
P13	**Personale e formazione**	Legale rappresentante	annuale	6.1-6.8	DORA artt. 13(6), 30(2)(i); AI Act art. 4; GDPR artt. 29, 32(4)
P14	**Uso accettabile**	Responsabile della sicurezza	annuale	5.10, 6.7, 8.1	DORA art. 9; L. 132/2025 art. 13; AI Act art. 50
P15	**Governance dell'intelligenza artificiale**	Responsabile della conformità IA, [nome]	annuale e a ogni cambio di modello, di fornitore o di finalità	5.1, 5.31, 5.34; ISO/IEC 42001 come riferimento	AI Act artt. 4, 5, 6, 25, 50, 53; L. 132/2025 art. 13; GDPR art. 22
P16	**Fascicoli penali**	DPO e Responsabile della sicurezza	annuale	5.12, 5.34, 8.3, 8.15	GDPR artt. 10, 35; art. 2-octies Codice privacy; artt. 114, 268, 269 c.p.p.
P17	**Gestione delle segnalazioni**	Gestore delle segnalazioni, [persona o soggetto esterno]	annuale	6.8	D.Lgs. 10 marzo 2023, n. 24; direttiva (UE) 2019/1937; GDPR

Regole comuni

Le eccezioni a qualsiasi politica seguono P01 § 8: richiesta scritta, valutazione del rischio con il metodo di P02, approvazione dell'organo amministrativo se il rischio residuo è alto o critico, registro delle eccezioni con scadenza, comunicazione al Cliente DORA interessato. Le violazioni seguono P01 § 9. Ogni politica è pubblicata anche come documento a sé, con lo stesso testo e lo stesso codice.

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.

POLITICA P02 · POL-02

Politica di gestione del rischio ICT

Il metodo unico con cui Trailgun governa i rischi per il servizio e per i dati dei Clienti, e il registro che ne risulta.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P02 (POL-02)	Responsabile della sicurezza	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
metodo annuale; registro ogni trimestre e a ogni evento rilevante	organo amministrativo; Responsabile della sicurezza; DPO; uffici ICT risk e audit dei Clienti	Riservato · per il Cliente

DOCUMENTI COLLEGATI

P01, P10; registro dei rischi ICT (41); inventario degli asset (42); registro dei subfornitori (15); documento 12 (Percorso di certificazione e piattaforma)

AMBITO

Tutti gli asset dell'inventario (42), i processi che li usano, i fornitori della politica P10 e i rischi legali e di conformità che derivano dal servizio, nei tre ambienti.

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
5.7, 5.9; clausole 6.1, 8.2, 8.3	DORA artt. 6, 8, 16, 28(4), 29; Reg. del. (UE) 2024/1774

1 Scopo e ambito

Questa politica dà ai Clienti che sono entità finanziarie le informazioni che servono al loro quadro di gestione del rischio TIC (artt. 6 e 8 DORA, o art. 16 per il quadro semplificato degli intermediari 106) e alla valutazione del rischio da terzi prima e durante il contratto (art. 28, par. 4, DORA). All'interno, governa con un metodo unico le priorità di Trailgun: ogni investimento in sicurezza parte da una voce del registro.

2 Ruoli

2.1 **Organo amministrativo.** Fissa la propensione al rischio (§ 6), approva i piani di trattamento dei rischi alti e critici e le accettazioni del rischio residuo alto, riceve la sintesi del registro con la relazione annuale.

2.2 **Responsabile della sicurezza.** Conduce il processo, tiene il registro (41) e l'inventario (42), assegna un titolare a ogni rischio e ne segue i trattamenti.

2.3 **DPO e responsabile della conformità IA.** Valutano, ciascuno per la sua materia, i rischi per i diritti degli interessati (dati giudiziari, cancellazione, trasferimenti) e i rischi propri dell'IA (errori, trasparenza, usi esclusi), e ne sono titolari nel registro.

3 Il processo

1 **Contesto e inventario.** Il Responsabile della sicurezza tiene l'inventario degli asset (42) e la mappa dei flussi dei dati, aggiornati a ogni cambiamento rilevante registrato nel registro dei cambiamenti (45).

2 **Identificazione.** Fonti: la rilevazione dello stato della piattaforma sul commit in production, gli incidenti e i quasi incidenti, le vulnerabilità, i cambi di fornitore, le novità normative, i rilievi degli audit dei Clienti, le informazioni sulle minacce.

3 **Analisi.** Ogni rischio ha uno scenario (causa, evento, effetto), i controlli in essere e un punteggio probabilità × impatto sulle scale del § 5, inerente e residuo.

4 **Valutazione.** Il punteggio residuo si confronta con la propensione al rischio (§ 6).

5 **Trattamento.** Ridurre con un controllo, evitare togliendo l'attività, trasferire (polizze, contratti con i fornitori), accettare. Ogni trattamento ha un titolare, una data e il punteggio residuo atteso; se il trattamento è una tappa del Percorso, il registro ne riporta il codice (R01–R17).

6 **Monitoraggio e riesame.** Lo stato dei trattamenti si verifica ogni trimestre; il registro si riesamina per intero ogni anno e dopo ogni incidente grave, vulnerabilità critica o cambiamento dell'architettura.

7 **Comunicazione.** Il Cliente DORA riceve su richiesta, sotto riservatezza, il registro o la sua sintesi per le voci che riguardano il suo servizio.

4 Inventario degli asset (sintesi)

L'inventario completo è il foglio 42. La sintesi qui sotto descrive production; development e staging hanno gli stessi componenti, separati, con dati e servizi esterni di prova.

ASSET	CHE COS'È	LUOGO	CLASSE (P11)
Istanza applicativa	EC2 Graviton, Amazon Linux 2023 aggiornato ogni mese, IMDSv2 obbligatorio; container dell'app (non root) e di Caddy (versione fissata)	eu-central-1	Strettamente riservato
Disco dati	EBS gp3 cifrato: database, originali, testi, indici, elaborati, faldoni, materiali, fatture	eu-central-1	Strettamente riservato
Copie di sicurezza	Snapshot giornalieri e prima di ogni rilascio, copie cifrate in Irlanda (politica P09)	eu-central-1, eu-west-1	Strettamente riservato
Archivio temporaneo	Bucket S3 per Textract e Transcribe, cifrato, privato, scadenza 1 giorno	eu-central-1	Strettamente riservato
Modelli	Claude su Amazon Bedrock (agenti); Amazon Titan Text Embeddings V2 su Bedrock (ricerca veloce)	regione UE	Strettamente riservato
Identità	Pool Amazon Cognito di production, TOTP obbligatorio; IAM Identity Center per il personale	eu-central-1	Riservato
Segreti	SSM Parameter Store (SecureString)	eu-central-1	Strettamente riservato
Registri	CloudWatch Logs (accessi e app, 90 giorni); CloudTrail con convalida dell'integrità (12 mesi); GuardDuty	eu-central-1	Riservato
Codice e CI	Repository GitHub privato, branch di ambiente protetti, GitHub Actions con OIDC; infrastruttura come codice (AWS CDK)	GitHub	Riservato, senza dati dei Clienti
Fornitori accessori	Posta, banca dati, firma e visure, notifiche, pagamenti: politica P10 e registro 15	secondo il fornitore	secondo il fornitore

5 Scale di misura

5.1 **Probabilità (P).** 1 rara: meno di una volta in cinque anni. 2 possibile: una volta in due-cinque anni. 3 probabile: almeno una volta all'anno. 4 quasi certa: attesa nell'anno, o condizione già in atto.

5.2 **Impatto (I)**, il più alto fra le dimensioni. 1 basso: nessun dato dei Clienti coinvolto, disservizio sotto l'ora. 2 medio: disservizio entro l'RTO, nessun dato esposto, scostamento contrattuale minore. 3 alto: disservizio oltre l'RTO, esposizione limitata di dati di uno studio, perdita oltre l'RPO, scostamento dal contratto o dal DPA. 4 molto alto: esposizione di dati giudiziari o di più studi, perdita estesa di dati, sanzioni o impossibilità per un Cliente di rispettare i propri obblighi di vigilanza.

5.3 **Punteggio** = P × I: da 1 a 3 basso, da 4 a 6 medio, 8 e 9 alto, 12 e 16 critico.

IMPATTO ↓ · PROBABILITÀ →	1 RARA	2 POSSIBILE	3 PROBABILE	4 QUASI CERTA
4 MOLTO ALTO	4 medio	8 alto	12 critico	16 critico
3 ALTO	3 basso	6 medio	9 alto	12 critico
2 MEDIO	2 basso	4 medio	6 medio	8 alto
1 BASSO	1 basso	2 basso	3 basso	4 medio

6 Propensione al rischio

6.1 **Critico:** non accettato. Il trattamento parte subito, lo approva l'organo amministrativo e, se tocca un impegno contrattuale, il rischio si comunica ai Clienti interessati.

6.2 **Alto:** accettato solo con un piano di trattamento datato, approvato dall'organo amministrativo.

6.3 **Medio:** accettato dal Responsabile della sicurezza, con monitoraggio a ogni trimestre.

6.4 **Basso:** accettato; si riesamina alla revisione annuale.

6.5 Nessun rischio che riguardi la riservatezza dei dati giudiziari (politica P16) si accetta oltre il livello medio.

7 Rischio da terzi e di concentrazione

Ogni fornitore della politica P10 è una voce dell'inventario e, se essenziale o importante, del registro dei rischi. Si valutano in particolare la dipendenza da un unico fornitore cloud (Amazon Web Services EMEA SARL, che le autorità europee di vigilanza hanno designato fornitore terzo critico il 18/11/2025), che con i modelli su Amazon Bedrock fornisce anche il servizio dei modelli; la catena di subfornitura; il luogo dei dati; la sostituibilità. La concentrazione su AWS è un rischio accettato e monitorato, mitigato dall'infrastruttura come codice, dai formati aperti dei dati, dal piano di uscita per fornitore (P10 § 7) e dal deposito del codice (Percorso, tappa R09). Le stesse informazioni servono al Cliente per la propria valutazione della concentrazione (art. 29 DORA).

8 Il registro dei rischi

Il registro è il foglio 41 (Registro dei rischi ICT): per ogni voce asset o processo, minaccia, vulnerabilità, probabilità e impatto, rischio inerente, controlli in essere, rischio residuo, titolare, trattamento, eventuale tappa del Percorso e data di riesame. Questa politica non lo ricopia: ne fissa il metodo. Il registro si aggiorna a ogni evento e si consegna ai Clienti DORA che lo chiedono, sotto riservatezza.

9 Trasferimento del rischio

Trailgun ha in essere una polizza cyber e una polizza di responsabilità civile professionale per errori e omissioni del software, con massimali di [€ ...] e [€ ...] per sinistro e per anno. Il certificato di assicurazione si consegna al Cliente che lo chiede. I contratti con i fornitori trasferiscono a loro gli obblighi di sicurezza e di notifica (P10 § 4).

10 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
Metodo e registro	IN ESSERE questa politica; registro dei rischi ICT (41) rivalutato sullo stato della piattaforma al 01/12/2026	riesame trimestrale e annuale; versione nel registro
Inventario degli asset	IN ESSERE foglio 42, dall'infrastruttura come codice	a ogni cambiamento rilevante
Approvazioni	IN ESSERE propensione al rischio e piani per i rischi alti	verbale dell'organo amministrativo, [data]
Polizze	IN ESSERE cyber e RC professionale	certificato su richiesta

11 Eccezioni e riferimenti normativi

Eccezioni secondo P01 § 8. Riferimenti: DORA artt. 6, 8, 16, 28, par. 4, e 29; Reg. del. (UE) 2024/1774 (in particolare art. 4 e, per il quadro semplificato, titolo III); ISO/IEC 27001:2022 clausole 6.1 e 8.2-8.3, controlli 5.7 e 5.9; ISO/IEC 27005 come guida di metodo.

POLITICA P03 · POL-03

Politica di controllo degli accessi

Chi accede a che cosa e come: utenti degli studi, personale di Trailgun, servizi e integrazione continua.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P03 (POL-03)	Responsabile della sicurezza	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale; accessi privilegiati ogni trimestre	personale e collaboratori; amministratori degli studi; uffici ICT risk e audit dei Clienti	Riservato · per il Cliente

DOCUMENTI COLLEGATI

P01, P04, P13; procedure 21 (Ingresso e uscita del personale), 22 (Revisione degli accessi), 23 (Gestione delle chiavi e dei segreti); modello 44 (Revisione degli accessi)

AMBITO

Gli accessi all'app, al backoffice, all'API pubblica e alle caselle email d'ingresso; gli accessi all'account AWS, a GitHub, a Google Workspace e alle console dei fornitori; i ruoli dei servizi e della CI.

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
5.15–5.18, 7.2, 8.2–8.5	DORA art. 9(4)(c)–(d); Reg. del. (UE) 2024/1774 artt. 19–21; GDPR art. 32

1 Scopo e principi

Un accesso si concede solo se serve al compito, al livello minimo, a un'identità personale riconducibile a una persona, con autenticazione a più fattori. Le regole le applica il server: l'interfaccia nasconde ciò che un ruolo non può fare, ma il controllo è sempre lato server, a ogni richiesta.

2 Ruoli

2.1 **Responsabile della sicurezza.** Concede, rivede e revoca gli accessi del personale, dei servizi e dei fornitori; tiene il registro degli accessi del personale al contenuto e il modello 44.

2.2 **Amministratore dello studio.** Concede, rivede e revoca gli accessi dei propri utenti dall'Organizzazione, ne sceglie il ruolo e configura la visibilità dei clienti dello studio.

3 Utenti degli studi

3.1 **Ingresso solo su invito** dell'amministratore dello studio o della piattaforma: non esiste registrazione libera. Il pool Amazon Cognito consente la creazione degli utenti solo agli amministratori.

3.2 **Autenticazione forte.** Protocollo SRP (la password non transita né si conserva presso Trailgun); password di almeno 10 caratteri con maiuscole, minuscole e cifre; password temporanea valida 7 giorni; messaggi che non rivelano l'esistenza di un utente; autenticazione a più fattori con app TOTP obbligatoria per tutti gli utenti.

3.3 **Verifica a ogni richiesta.** Ogni chiamata a `/api/*` verifica il token d'identità (firma sulle chiavi del pool, scadenza, destinatario) e confronta l'utente della richiesta con quello del token.

3.4 **Ruoli dello studio. admin** (vede l'Organizzazione), **membro**, **operator** (porta avanti le pratiche esistenti, non ne crea di nuove) e **viewer** (sola lettura: nessuna scrittura, niente assistente, niente esportazione in Word). Le regole dei ruoli stretti stanno in un solo punto del codice e valgono per ogni richiesta. Permessi aggiuntivi per singolo membro: richiesta di attenzione e Amministrazione.

3.5 **Visibilità per cliente.** Ogni cliente dello studio è visibile a tutto lo studio, solo a chi l'ha creato o a persone selezionate. Un unico predicato decide la visibilità di ogni dato di un cliente, coperto da test sull'isolamento fra studi.

3.6 **Chiavi API dello studio.** Agiscono per conto di un utente; se ne conservano solo l'hash SHA-256 e il prefisso; limite di 120 richieste al minuto per chiave; revoca immediata dall'Organizzazione; rotazione consigliata ogni 12 mesi, a cura dello studio.

3.7 **Caselle email d'ingresso.** Ogni casella ha un token; le mail da mittenti non riconosciuti restano trattenute finché un utente non le approva; le mail di operatori e viewer non aprono pratiche.

3.8 **Sessione e disattivazione.** Il token d'identità ha una scadenza breve, [1 ora]. La disattivazione di un utente blocca subito i nuovi accessi; una sessione già aperta termina alla scadenza del token.

4 Personale di Trailgun

4.1 **Backoffice.** Protetto dal login Cognito con autenticazione a più fattori e dall'appartenenza al gruppo `admin`. L'amministratore della piattaforma vede studi, utenti, impostazioni, prompt e i metadati di pratiche e costi (titoli, stati, importi), mai il contenuto delle pratiche: il predicato di visibilità vale anche per lui.

4.2 **Assistenza.** Il gruppo `supporto` vede solo i ticket e la knowledge base.

4.3 **Accesso al contenuto.** Il personale accede al contenuto di una pratica solo su richiesta del Cliente o per gestire un incidente. Ogni accesso si annota nel registro degli accessi del personale con richiedente, motivo, dati consultati, inizio e fine; il Cliente interessato ne riceve l'estratto su richiesta.

4.4 **Infrastruttura.** L'accesso alla macchina e ai dati del volume è riservato a chi ne ha bisogno per gestire la piattaforma, con credenziali temporanee e sessioni registrate (§ 5); l'elenco nominativo è nel modello 44 e si rivede ogni trimestre.

5 Accessi privilegiati e autenticazione forte

5.1 Autenticazione a più fattori obbligatoria su AWS (utente root e console), GitHub (obbligo a livello di organizzazione), Google Workspace, Stripe, Resend e ogni console di fornitore.

5.2 Agli accessi amministrativi ad AWS si accede solo con credenziali temporanee di AWS IAM Identity Center, legate alla persona: nessuna chiave d'accesso statica.

5.3 L'utente root dell'account AWS non si usa per l'operatività: credenziali e dispositivo MFA sono custoditi come accesso di emergenza, il cui uso si registra (CloudTrail) e si comunica all'organo amministrativo.

5.4 Nessun accesso SSH: l'istanza non ha la porta 22 aperta e si amministra con AWS Systems Manager; ogni sessione si registra e si conserva 12 mesi (politica P08).

6 Servizi e integrazione continua

6.1 L'istanza ha un ruolo a privilegi limitati: lettura delle immagini, scrittura dei log, bucket temporaneo, Textract e Transcribe, modelli su Bedrock nelle sole regioni UE, parametri del proprio prefisso, gestione degli utenti del proprio pool.

6.2 GitHub Actions non ha chiavi AWS: ogni ambiente ha un ruolo OIDC assumibile solo dal branch omonimo, limitato al proprio ambiente; l'infrastruttura non si modifica dalla CI.

6.3 I segreti dei fornitori stanno in SSM Parameter Store cifrato, mai nel codice o nell'immagine; si ruotano ogni 12 mesi e subito dopo un sospetto di compromissione o l'uscita di una persona che vi aveva accesso (procedura 23).

7 Ciclo di vita degli accessi

1 **Richiesta.** Chi ha bisogno di un accesso lo chiede al Responsabile della sicurezza con il motivo e il livello; per l'ingresso di una persona vale la procedura 21.

2 **Condizioni.** Impegno di riservatezza, designazione al trattamento, verifica dei precedenti per chi accede alla produzione, formazione all'ingresso (politica P13).

3 **Concessione.** Identità personale, livello minimo, autenticazione a più fattori attiva prima del primo uso; l'accesso si annota con data e approvatore.

4 **Cambio di ruolo.** Gli accessi del ruolo precedente si revocano nello stesso giorno in cui si concedono i nuovi.

5 **Revisione trimestrale.** Accessi privilegiati (AWS, GitHub, backoffice, gruppi Cognito `admin` e `supporto`, Google Workspace, console dei fornitori) e account di servizio, secondo la procedura 22; esito e correzioni nel modello 44; ogni accesso non più giustificato si revoca.

6 **Uscita.** Revoca di tutti gli accessi entro 24 ore dalla cessazione del rapporto, rotazione dei segreti a cui la persona aveva accesso, verbale (procedura 21).

8 Accesso fisico

Trailgun non ha sale server: i sistemi sono nei data center di Amazon Web Services, la cui sicurezza fisica è attestata nei rapporti ISO/IEC 27001 e SOC 2 di AWS, disponibili su richiesta tramite AWS Artifact. I dispositivi del personale seguono la politica P14.

9 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
MFA per gli utenti	IN ESSERE TOTP obbligatorio nel pool di production	configurazione del pool

CONTROLLO	EVIDENZA	DOVE E QUANDO
Verifica del token, ruoli, visibilità, chiavi API	IN ESSERE applicati lato server, con test automatici	a ogni verifica della CI
MFA e credenziali temporanee per il personale	IN ESSERE IAM Identity Center; MFA su tutte le console; 2FA obbligatoria su GitHub	modello 44
Sessioni sulla macchina	IN ESSERE sessioni SSM registrate	12 mesi (P08)
Registro degli accessi del personale	IN ESSERE ogni accesso al contenuto con motivo e durata	a ogni accesso; estratto al Cliente su richiesta
Revisione degli accessi	IN ESSERE trimestrale, prima revisione verbalizzata il [data]	modello 44, ogni trimestre

10 Eccezioni e riferimenti normativi

Eccezioni secondo P01 § 8; nessuna eccezione all'autenticazione a più fattori sugli accessi privilegiati. Riferimenti: DORA art. 9, par. 4, lett. c) e d); Reg. del. (UE) 2024/1774 artt. 19-21 (identità unica e autenticazione forte del personale del fornitore); GDPR art. 32; ISO/IEC 27001:2022 controlli 5.15-5.18, 7.2, 8.2-8.5.

POLITICA P04 · POL-04

Politica di crittografia e gestione delle chiavi

Che cosa si cifra, con quali algoritmi, chi custodisce le chiavi e come si ruotano.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P04 (POL-04)	Responsabile della sicurezza	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale e a ogni cambio di algoritmo o servizio	personale tecnico; uffici ICT risk e CISO dei Clienti	Riservato · per il Cliente

DOCUMENTI COLLEGATI
P03, P09, P11; procedura 23 (Gestione delle chiavi e dei segreti); procedura 28 (Restituzione e cancellazione a fine contratto)

AMBITO
Dati a riposo e in transito della piattaforma, copie di sicurezza, segreti, chiavi API, firme dei webhook, esportazioni verso i Clienti.

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
8.24, 5.17, 8.20, 8.21	DORA art. 9(4)(d); Reg. del. (UE) 2024/1774 art. 6; GDPR art. 32(1)(a)

1 Scopo e ruoli

La cifratura protegge i dati dei Clienti quando un altro controllo cede: un supporto smarrito, una copia trasferita, una connessione intercettata. Il Responsabile della sicurezza sceglie algoritmi e servizi, custodisce le chiavi e i segreti e ne tiene l'inventario (procedura 23); le chiavi KMS sono gestite dal servizio AWS Key Management Service e non escono mai in chiaro.

2 Dati a riposo

2.1 Il disco dati e il disco di sistema di ogni istanza sono volumi EBS cifrati con AES-256 tramite AWS KMS. Gli snapshot e le loro copie in Irlanda sono cifrati.

2.2 Il bucket temporaneo per Textract e Transcribe usa la cifratura lato server (SSE-S3), blocca l'accesso pubblico, accetta solo connessioni TLS e cancella gli oggetti entro 1 giorno; l'app li cancella a fine analisi.

2.3 I segreti sono SecureString in SSM Parameter Store, cifrati con KMS; sul server il file di configurazione è leggibile solo dal servizio.

2.4 La protezione a riposo è quella del volume e delle copie: database e file non hanno una seconda cifratura applicativa. Per questo chi può accedere al sistema in esecuzione è regolato dalla politica P03 (credenziali temporanee, sessioni registrate, registro degli accessi del personale).

2.5 Le chiavi KMS sono gestite da AWS, con rotazione annuale automatica. Le chiavi gestite da Trailgun (KMS CMK) per volumi, database e file fanno parte della nuova piattaforma (Percorso, tappa R12).

3 Dati in transito

3.1 Tutto il traffico pubblico passa da HTTPS con TLS 1.2 o superiore (1.3 preferito), HTTP/3, reindirizzamento da HTTP a HTTPS, HSTS di un anno e intestazioni di sicurezza (CSP, X-Content-Type-Options, Referrer-Policy, frame-ancestors). I certificati sono di Let's Encrypt e si rinnovano automaticamente; la loro scadenza è sotto allarme.

3.2 Le chiamate ai fornitori (AWS, posta, firma, banche dati) usano sempre HTTPS; le richieste ai modelli su Amazon Bedrock sono firmate con SigV4 dal ruolo dell'istanza, senza chiavi su disco.

3.3 I webhook in uscita verso i sistemi degli studi sono firmati HMAC-SHA256 con timestamp (`Trailgun-Signature`); quelli in entrata si verificano con Svix (tolleranza 5 minuti) o con un segreto condiviso, e senza segreto la rotta risponde 503.

3.4 Ogni consegna di dati a un Cliente fuori dall'app, compresa l'esportazione complessiva a fine contratto, avviene in un archivio cifrato tramite un link temporaneo; l'indice dei file porta le impronte SHA-256 (procedura 28; esportazione in autonomia: Percorso, tappa R02).

4 Algoritmi

4.1 **Ammessi:** AES-256 per la cifratura simmetrica; TLS 1.2 e 1.3 con suite AEAD; SHA-256 o superiore per impronte e hash; HMAC-SHA256 per le firme; SRP per l'autenticazione degli utenti; SigV4 per le richieste ai servizi AWS.

4.2 **Vietati** per scopi di sicurezza: MD5, SHA-1, TLS inferiore a 1.2, algoritmi o implementazioni crittografiche scritti in proprio. Le librerie crittografiche sono quelle della piattaforma (Node.js, AWS).

4.3 Le chiavi API degli studi si conservano solo come hash SHA-256; le password non si conservano mai presso Trailgun; i file del pacchetto di deposito portano l'impronta SHA-256.

5 Chiavi e segreti

ELEMENTO	ROTAZIONE	CUSTODE
Chiavi KMS	annuale automatica	AWS KMS
Segreti dei fornitori	ogni 12 mesi e subito dopo un sospetto di compromissione o l'uscita di una persona con accesso; data annotata nell'inventario	Responsabile della sicurezza (SSM)
Certificati TLS	automatica (Let's Encrypt, 90 giorni), scadenza sotto allarme	Caddy
Chiavi API degli studi	a cura dello studio, consigliata ogni 12 mesi; revoca immediata	lo studio (Trailgun conserva solo l'hash)
Credenziali del personale	temporanee, a ogni sessione (IAM Identity Center)	la persona

5.1 Un segreto non si trasmette mai per email o chat in chiaro, non si scrive nei log e non entra nel repository: la scansione dei segreti (gitleaks) controlla tutta la storia del repository a ogni verifica della CI.

5.2 Un segreto esposto si revoca e si ruota subito, si toglie dalla storia del repository e l'evento si tratta come incidente (procedura 23 e procedura 25).

6 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
Cifratura dei volumi e delle copie	IN ESSERE volumi e snapshot cifrati in Germania e in Irlanda	infrastruttura come codice; inventario 42
TLS, HSTS e intestazioni	IN ESSERE configurazione del proxy	verificabile dall'esterno su app.trailgun.ai
Inventario e rotazione dei segreti	IN ESSERE data di creazione e ultima rotazione di ogni segreto	procedura 23; riesame annuale
Scansione dei segreti	IN ESSERE job «secrets» della verifica della CI	a ogni pull request e prima di ogni rilascio

7 Eccezioni e riferimenti normativi

Eccezioni secondo P01 § 8; nessuna eccezione ammette un algoritmo vietato. Riferimenti: DORA art. 9, par. 4, lett. d); Reg. del. (UE) 2024/1774 art. 6; GDPR art. 32, par. 1, lett. a); ISO/IEC 27001:2022 controlli 8.24, 5.17, 8.20 e 8.21.

POLITICA P05 · POL-05

Politica di sicurezza delle operazioni e gestione dei cambiamenti

Ambienti, configurazione, capacità e rilasci: come ogni cambiamento arriva in production senza sorprese per i Clienti.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P05 (POL-05)	Responsabile della sicurezza	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale	personale tecnico; uffici ICT risk e audit dei Clienti	Riservato · per il Cliente

DOCUMENTI COLLEGATI

P06, P07, P09; procedura 20 (Gestione dei cambiamenti); registro dei cambiamenti (45); documento 11 (Continuità operativa, ripristino e incidenti)

AMBITO

Codice dell'app, immagini dei container, infrastruttura (AWS CDK), configurazione e segreti, prompt del registro, modelli assegnati agli agenti, fornitori collegati.

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
5.37, 8.6, 8.7, 8.9, 8.19, 8.31, 8.32	DORA art. 9(4)(e); Reg. del. (UE) 2024/1774

1 Scopo e ruoli

Un servizio stabile nasce da ambienti separati, da una configurazione descritta come codice e da cambiamenti che seguono sempre lo stesso percorso. Il Responsabile della sicurezza approva i cambiamenti dell'infrastruttura e i cambiamenti urgenti, tiene il registro dei cambiamenti (45) e decide le finestre di manutenzione; chi sviluppa apre la pull request e ne risponde.

2 Ambienti

2.1 Tre ambienti online, ciascuno con il proprio stack, la propria macchina, il proprio disco, IP, registro delle immagini, parametri, log, bucket e pool di utenti: development (app.dev.trailgun.ai), staging (app.staging.trailgun.ai), production (app.trailgun.ai).

2.2 Development e staging usano di default servizi esterni di prova (banca dati, posta, notifiche, firma). Lo script di rilascio impone a ciascun ambiente il pool di utenti del suo stack, così una configurazione copiata da production non fa entrare gli utenti veri.

2.3 I dati di production non si copiano negli altri ambienti né sui computer del personale. Prove e dimostrazioni usano dati sintetici.

3 Configurazione e capacità

3.1 L'infrastruttura è descritta come codice (AWS CDK) ed è ricostruibile. L'immagine del sistema operativo dell'istanza riceve gli aggiornamenti di sicurezza ogni mese; l'immagine del proxy Caddy è fissata a una versione e si aggiorna con un cambiamento ordinario; il container dell'app gira con un utente non privilegiato.

3.2 Spazio disco, CPU, memoria, errori 5xx e scadenza dei certificati sono sotto allarme 24/7 (politica P08). Le immagini conservate nel registro sono le ultime 15; le copie del database prima delle migrazioni sono le ultime 5.

4 Tipi di cambiamento

4.1 **Ordinario: rilascio dell'app.** Branch di lavoro, pull request verso development, poi promozione per branch di ambiente: staging, production. I branch di ambiente sono protetti: si aggiornano solo con pull request e con la verifica superata. Una promozione diretta da development a production segue le stesse regole e si annota nel registro.

4.2 **Infrastruttura.** `cdk deploy` solo a mano, con lo stack nominato, approvato dal Responsabile della sicurezza; mai dalla CI.

4.3 **Prompt e modelli.** Il testo dei prompt si cambia solo dal backoffice della piattaforma e non esce mai verso il browser di uno studio; lo studio può solo aggiungere testi propri. Un cambio del modello predefinito di un agente è un cambiamento rilevante (politica P15).

4.4 **Urgente** (sicurezza, ripristino). Si esegue subito, si documenta nel registro entro il giorno lavorativo successivo con motivo e verifica, e si comunica ai Clienti come intervento urgente.

5 Il percorso di un rilascio

1. **Verifica obbligatoria.** Controllo dei tipi del server, del frontend e dell'infrastruttura; test unitari; test end-to-end dell'interfaccia; scansione dei segreti su tutta la storia del repository; prova di ripristino del database. Se uno di questi passi fallisce, il rilascio non parte.
2. **Immagine.** Costruita in CI con il commit come etichetta e analizzata dal registro delle immagini al caricamento.
3. **Production solo dal suo branch.** Il rilascio di production parte solo dal branch `production` e rifiuta un commit che non ha superato la verifica, anche quando è lanciato a mano.
4. **Copia prima del rilascio.** Il disco dati si fotografa (snapshot con il commit come etichetta, conservato 14 giorni).
5. **Nessuna lavorazione interrotta.** Il rilascio si rifiuta se ci sono atti del modulo in lavorazione; forzarlo è un cambiamento urgente da documentare. Le lavorazioni in coda ripartono da sole.
6. **Migrazioni.** All'avvio l'app applica le migrazioni del database: numerate, solo in avanti, mai modificate dopo la pubblicazione e compatibili con l'immagine precedente, così il ritorno all'immagine precedente non richiede di toccare i dati.
7. **Controllo di salute.** Il rilascio verifica `/api/health` prima di dichiararsi concluso; la riga del registro dei cambiamenti riporta esito e snapshot.

6 Finestre e comunicazione

La manutenzione programmata si annuncia con almeno 48 ore di preavviso, si svolge tra le 20:00 e le 07:00 o nel fine settimana, per non più di 8 ore al mese, mai nella finestra lavorativa. I rilasci ordinari durano meno di 2 minuti e avvengono solo senza lavorazioni del modulo in corso; una lavorazione interrotta si riavvia senza costi. I cambi di subfornitori seguono i preavvisi della politica P10.

7 Protezione dal codice malevolo

I file caricati non si eseguono mai: si leggono e si convertono con componenti dedicati (pdf.js, LibreOffice, Chromium) nel container dell'app, che gira senza privilegi. Gli archivi hanno limiti sul numero di voci (5.000) e sulla dimensione contro gli zip bomb. Il penetration test indipendente (Percorso, tappa R06) verifica anche questi percorsi; il filtro applicativo (WAF) arriva con la nuova piattaforma (tappa R12).

8 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
Ambienti separati, infrastruttura come codice	IN ESSERE tre stack, un pool di utenti ciascuno	repository dell'infrastruttura
Branch protetti e verifica obbligatoria	IN ESSERE anche per il rilascio di production lanciato a mano	esito della verifica nella pull request
Snapshot prima del rilascio	IN ESSERE con il commit come etichetta, 14 giorni	a ogni rilascio di production
Registro dei cambiamenti	IN ESSERE pull request, tipo, verifica, approvazione, migrazione, snapshot, esito	foglio 45, a ogni rilascio
Aggiornamenti del sistema e del proxy	IN ESSERE immagine aggiornata ogni mese; Caddy a versione fissata; container non root	registro dei cambiamenti

9 Eccezioni e riferimenti normativi

Eccezioni secondo P01 § 8; nessuna eccezione ammette un rilascio di production senza verifica superata. Riferimenti: DORA art. 9, par. 4, lett. e); Reg. del. (UE) 2024/1774; ISO/IEC 27001:2022 controlli 5.37, 8.6, 8.7, 8.9, 8.19, 8.31, 8.32.

POLITICA P06 · POL-06

Politica di sviluppo sicuro

Le regole con cui Trailgun progetta, scrive, prova, rivede e pubblica il software.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P06 (POL-06)	Responsabile della sicurezza	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale	chi sviluppa per Trailgun; uffici ICT risk e CISO dei Clienti	Riservato · per il Cliente

DOCUMENTI COLLEGATI

P05, P07, P15; procedura 20 (Gestione dei cambiamenti); procedura 23 (Gestione delle chiavi e dei segreti); documento 57 (Deposito del codice: term sheet)

AMBITO

Tutto il codice di Trailgun (app, frontend, infrastruttura, script), le dipendenze, i prompt del registro e gli strumenti di sviluppo, compresi gli assistenti di programmazione basati su IA.

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
8.4, 8.25-8.30, 8.33	Reg. del. (UE) 2024/1774 art. 16; DORA art. 25; GDPR art. 25

1 Scopo e ruoli

La sicurezza del servizio si decide quando si scrive il codice. Questa politica vale per chiunque scriva codice per Trailgun; il Responsabile della sicurezza ne verifica il rispetto e approva le eccezioni.

2 Requisiti e progettazione

2.1 Ogni funzione nuova nasce come opzione, attivabile dalle impostazioni e nel modulo dell'atto; spenta, il flusso resta identico, stesso percorso e stessi prompt; la scelta si congela sull'atto alla creazione.

2.2 Punti unici per le operazioni sensibili: ogni atto nasce da una sola funzione (`creaAtto`); il testo dell'atto si scrive da una sola funzione (`scriviTestoAtto`), che conserva le versioni con autore e motivo; la visibilità dei dati di un cliente passa da un solo predicato; le regole dei ruoli stretti stanno in un solo punto. Una funzione nuova riusa questi punti e non li aggira.

2.3 Ogni uscita nuova verso lo studio (JSON, stream, file, email, risposte degli agenti) rispetta le regole sui dati e sui costi: un campo nuovo con un dato riservato si aggiunge ai filtri esistenti e ha un test.

2.4 Un passo accessorio non fa mai fallire l'atto: a ogni guasto resta il risultato precedente.

2.5 Privacy fin dalla progettazione: si raccoglie e si conserva solo ciò che serve; nessun testo dei documenti nei log o nei registri dei costi; sui fascicoli penali nessun embedding (politica P16).

3 Scrittura del codice

3.1 TypeScript con controllo dei tipi obbligatorio, formattazione uniforme, schema del database cambiato solo con migrazioni numerate.

3.2 Nessun segreto nel repository, nell'immagine o nel template dell'infrastruttura. La scansione dei segreti (gitleaks, con le regole predefinite e le sole eccezioni motivate per falsi positivi) controlla l'intera storia del repository a ogni verifica della CI; un segreto trovato si ruota e si toglie dalla storia, mai si mette in eccezione.

3.3 I prompt stanno solo nel registro dei prompt, non sparsi nel codice; ogni prompt ha una sintesi obbligatoria.

3.4 Gli assistenti di programmazione basati su IA lavorano sul codice sotto il controllo dello sviluppatore, che ne risponde. Il repository non contiene dati dei Clienti e agli assistenti non si danno dati dei Clienti, documenti delle pratiche o segreti.

3.5 Le dipendenze si aggiornano con le richieste settimanali di Dependabot (npm dell'app e dell'infrastruttura, immagini Docker, GitHub Actions), integrate dopo la verifica; gli strumenti scaricati dalla CI sono a versione fissata e controllati con l'impronta SHA-256.

4 Prove

4.1 Ogni pull request verso un branch di ambiente e ogni rilascio superano: controllo dei tipi (server, frontend, infrastruttura), test unitari, test end-to-end, scansione dei segreti e prova di ripristino del database (copie ripristinate e verificate con controllo d'integrità, schema, righe e file).

4.2 Le aree sensibili hanno test dedicati: verifica dei token, isolamento fra studi, ruoli, API pubblica e chiavi, regole sui costi visibili allo studio, marcatura dei contenuti generati, esclusione delle regioni fuori dall'UE.

4.3 Le prove usano dati sintetici, mai dati di production.

4.4 Le prove di sicurezza indipendenti seguono il Percorso: scansione esterna mensile dell'applicazione (tappa R05) e penetration test annuale e dopo ogni cambiamento rilevante dell'architettura (tappa R06).

5 Revisione e pubblicazione

Ogni modifica entra con una pull request verso un branch di ambiente protetto: la verifica deve essere superata prima dell'integrazione, e la revisione del codice si fa con strumenti di revisione automatica e con la lettura dello sviluppatore responsabile. La pubblicazione segue la politica P05. Il codice sorgente e le istruzioni di ricostruzione si depositano presso un agente terzo con aggiornamento trimestrale (Percorso, tappa R09; documento 57).

6 Sviluppo affidato a terzi

Trailgun sviluppa il proprio codice. Se affida parte dello sviluppo a terzi, il fornitore riceve questa politica per contratto, non ha accesso alla produzione né ai dati dei Clienti e il suo codice passa dalla stessa verifica e dalla stessa pull request.

7 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
Verifica obbligatoria	IN ESSERE tipi, test unitari ed end-to-end, segreti, prova di ripristino	esito in ogni pull request; registro 45
Scansione dei segreti	IN ESSERE gitleaks sull'intera storia, eccezioni motivate nella configurazione	a ogni verifica
Dipendenze e immagini	IN ESSERE Dependabot settimanale; scansione delle immagini al caricamento	tempi della politica P07
Container non root	IN ESSERE utente non privilegiato nell'immagine	a ogni immagine

8 Eccezioni e riferimenti normativi

Eccezioni secondo P01 § 8; nessuna eccezione ammette dati dei Clienti nel repository o nelle prove. Riferimenti: Reg. del. (UE) 2024/1774 art. 16; DORA art. 25; GDPR art. 25; ISO/IEC 27001:2022 controlli 8.4, 8.25-8.30, 8.33.

POLITICA P07 · POL-07

Politica di gestione delle vulnerabilità

Come Trailgun scopre, valuta e corregge le vulnerabilità, con quali tempi, e come le comunica.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P07 (POL-07)	Responsabile della sicurezza	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale	personale tecnico; uffici ICT risk e CISO dei Clienti; ricercatori di sicurezza	Riservato · per il Cliente

DOCUMENTI COLLEGATI

P05, P06, P08; procedura 24 (Gestione delle vulnerabilità e segnalazione responsabile); procedura 25 (Risposta agli incidenti); documento 12 (Percorso di certificazione e piattaforma)

AMBITO

Componenti in uso nella piattaforma: codice, dipendenze, immagini dei container, sistema operativo dell'host, proxy Caddy, servizi AWS configurati da Trailgun.

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
8.8, 5.7, 6.8	DORA artt. 9(4)(f), 25; Reg. del. (UE) 2024/1774 art. 10

1 Scopo e ruoli

Una vulnerabilità nota e non corretta è il modo più comune in cui un servizio viene violato. Il Responsabile della sicurezza valuta ogni vulnerabilità, ne decide la gravità e il trattamento e verifica che i tempi del § 3 siano rispettati; chi sviluppa prepara la correzione con un cambiamento ordinario o urgente (politica P05).

2 Fonti

- Dependabot, settimanale, su tutte le dipendenze; scansione di ogni immagine al caricamento nel registro delle immagini.
- Scansione dei segreti (gitleaks) sull'intera storia del repository a ogni verifica della CI.
- Bollettini dei fornitori (AWS, Node.js, Caddy, LibreOffice, Chromium) e catalogo CISA delle vulnerabilità sfruttate (KEV).
- Segnalazioni esterne a security@trailgun.ai, secondo la politica di segnalazione responsabile pubblicata su https://trailgun.ai/security e in https://trailgun.ai/.well-known/security.txt (procedura 24); segnalazioni dei Clienti.
- Prove indipendenti: scansione esterna mensile dell'applicazione e penetration test annuale (Percorso, tappe R05 e R06).

3 Valutazione e tempi di correzione

La gravità si misura con CVSS v3.1 o v4. I tempi decorrono dalla disponibilità della correzione, per vulnerabilità che toccano componenti in uso. Se la correzione non c'è, si adotta subito una mitigazione (configurazione, disattivazione della funzione, regola di rete) e la si registra.

GRAVITÀ	CRITERIO	TEMPO MASSIMO	NOTE
Critica	CVSS ≥ 9,0 o sfruttata attivamente (KEV)	72 ore	mitigazione immediata se manca la correzione; valutazione come minaccia per i Clienti
Alta	CVSS 7,0-8,9	7 giorni	
Media	CVSS 4,0-6,9	30 giorni	
Bassa	CVSS < 4,0	90 giorni	
Sistema dell'host	aggiornamenti di sicurezza dell'immagine del sistema operativo	ogni mese	e subito, come critica, per una vulnerabilità critica del sistema

4 Il trattamento di una vulnerabilità

1. **Ricezione.** Ogni segnalazione o avviso si apre come voce di lavoro con fonte, componente e data di disponibilità della correzione.
2. **Valutazione.** Il Responsabile della sicurezza conferma se il componente è in uso e raggiungibile, assegna la gravità e il termine del § 3.

3 **Correzione o mitigazione.** Aggiornamento con un cambiamento ordinario o, per le critiche, urgente (politica P05); se la correzione manca, mitigazione registrata.

4 **Verifica.** La verifica della CI e la nuova scansione dell'immagine confermano la chiusura.

5 **Comunicazione.** Ai Clienti secondo il § 5; al segnalatore secondo la procedura 24.

5 Comunicazione

5.1 Una vulnerabilità che può riguardare un Cliente si tratta come minaccia informatica significativa e gli si comunica entro 24 ore; se è stata sfruttata, è un incidente (procedura 25).

5.2 Il rispetto dei tempi di correzione è nel rapporto di servizio (Percorso, tappa R04) e si comunica al Cliente che lo chiede; al Cliente si consegna, sotto riservatezza, la sintesi dei risultati del penetration test e il piano di rimedio.

5.3 Trailgun partecipa, alle condizioni concordate per non mettere a rischio gli altri clienti, ai test guidati dalla minaccia (TLPT) dei Clienti DORA (art. 26 DORA).

6 Segnalazione responsabile

Chi trova una vulnerabilità scrive a security@trailgun.ai. Trailgun conferma la ricezione, valuta e comunica l'esito, e non agisce contro chi segnala in buona fede senza accedere ai dati di altri, senza degradare il servizio e senza divulgare prima della correzione. Ambito, regole e tempi di risposta sono nella procedura 24, che riporta anche il testo pubblicato di security.txt.

7 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
Dependabot e scansione delle immagini	IN ESSERE avvisi e richieste di aggiornamento	settimanale; a ogni immagine
Tempi di correzione	IN ESSERE data di apertura, gravità, termine e chiusura di ogni voce	registro dei cambiamenti (45)
Aggiornamento mensile del sistema	IN ESSERE nuova immagine del sistema operativo ogni mese	registro dei cambiamenti
Segnalazione responsabile	IN ESSERE security.txt e pagina /security pubblicati	trailgun.ai; scadenza di security.txt rinnovata ogni anno

8 Eccezioni e riferimenti normativi

Eccezioni secondo P01 § 8: una correzione rinviata oltre i tempi richiede una mitigazione registrata e, per le critiche e le alte, l'approvazione del Responsabile della sicurezza con una nuova data. Riferimenti: DORA art. 9, par. 4, lett. f), e artt. 25-26; Reg. del. (UE) 2024/1774 art. 10; ISO/IEC 27001:2022 controlli 5.7, 6.8 e 8.8; RFC 9116 (security.txt).

POLITICA P08 · POL-08

Politica di logging e monitoraggio

Che cosa si registra, per quanto tempo, come si protegge, chi lo guarda e quando suona un allarme.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P08 (POL-08)	Responsabile della sicurezza	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale	personale tecnico; amministratori degli studi; uffici ICT risk e audit dei Clienti	Riservato · per il Cliente

DOCUMENTI COLLEGATI

P03, P12, P16; procedura 25 (Risposta agli incidenti); documento 11 (Continuità operativa, ripristino e incidenti); documento 55 (Accordo sul livello di servizio)

AMBITO

Log applicativi, di accesso, di sicurezza e di amministrazione della piattaforma; registri consultabili dagli studi; monitoraggio della disponibilità e degli allarmi.

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
8.15, 8.16, 8.17	DORA art. 10; Reg. del. (UE) 2024/1774 art. 12; GDPR art. 32

1 Scopo e ruoli

I log servono a rilevare le anomalie, a ricostruire un incidente e a dimostrare chi ha fatto che cosa. Il Responsabile della sicurezza decide che cosa si registra, ne protegge l'integrità, riceve gli allarmi ed esamina gli eventi di sicurezza; l'amministratore dello studio consulta ed esporta i registri dello studio.

2 Che cosa si registra e per quanto

REGISTRO	CONTENUTO	CONSERVAZIONE
Accessi HTTP	richieste al proxy: ora, indirizzo, metodo, percorso, esito, durata; mai corpo delle richieste né token	90 giorni, CloudWatch Logs
Applicativi	moduli, identificativi, nomi di file, errori; mai testo dei documenti	90 giorni, CloudWatch Logs
Sicurezza e amministrazione	CloudTrail in tutte le regioni con convalida dell'integrità; sessioni SSM sulla macchina; accessi al backoffice; risultati di GuardDuty	12 mesi
Attività dello studio	chi, che cosa, quando, su quale cliente o atto	per la durata del contratto; esportabile dall'amministratore dello studio
Accessi ai fascicoli penali	consultazioni (una all'ora per utente), domande, analisi, confronti fra depositi, timeline, grafi e schede dell'imputato generati	per la durata del contratto; esportabile dal Titolare
Accessi del personale al contenuto	richiedente, motivo, pratica, inizio e fine (politica P03)	per la durata del contratto; estratto al Cliente su richiesta
Costi	modello, agente, token, importo; mai il testo	per la fatturazione; scollegati dai contenuti alla cancellazione

3 Regole sul contenuto

3.1 I log non contengono testo dei documenti, corpo delle richieste, token, password o segreti. Un messaggio di log nuovo che potrebbe contenerli non supera la revisione del codice (politica P06).

3.2 I registri consultabili dagli studi seguono la stessa visibilità dei dati a cui si riferiscono e si cancellano con lo studio alla cessazione (politica P12).

3.3 Gli orologi sono sincronizzati con Amazon Time Sync Service (chrony, predefinito di Amazon Linux 2023), così gli eventi di sistemi diversi si confrontano sullo stesso tempo.

4 Protezione

I log di sicurezza e amministrazione si conservano con la convalida dell'integrità di CloudTrail e con accesso limitato al Responsabile della sicurezza; ogni modifica o cancellazione di un gruppo di log o di una traccia resta registrata in CloudTrail.

5 Monitoraggio e allarmi

5.1 Una sonda esterna controlla ogni minuto `https://app.trailgun.ai/api/health` e l'avvio di una lavorazione: è la misura della disponibilità dell'accordo sul livello di servizio (documento 55).

5.2 Allarmi 24/7 su salute dell'app, spazio disco, CPU, memoria, errori 5xx e scadenza dei certificati; GuardDuty segnala attività sospette sull'account.

5.3 Un allarme raggiunge il reperibile per telefono ed email; ogni allarme si valuta come possibile incidente secondo la procedura 25 e si annota con l'esito.

5.4 Gli eventi di sicurezza (GuardDuty, accessi amministrativi, uso dell'utente root) si esaminano a ogni allarme e, in blocco, a ogni revisione trimestrale degli accessi (procedura 22).

5.5 La pagina «Sistema» del backoffice mostra versione, dimensioni dei database, stato delle migrazioni e spazio disco.

5.6 La scrittura del registro degli accessi penali non blocca mai il lavoro dell'avvocato: se fallisce, l'errore va nei log applicativi e si esamina con gli altri errori.

6 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
Log di accesso e applicativi	IN ESSERE gruppi di log con conservazione di 90 giorni	CloudWatch Logs, eu-central-1
CloudTrail, GuardDuty, sessioni SSM	IN ESSERE traccia multi-regione con convalida dell'integrità, 12 mesi	account AWS di Trailgun
Sonda e allarmi	IN ESSERE sonda ogni minuto; allarmi su salute, disco, CPU, memoria, 5xx, certificati	prova di un allarme a ogni riesame annuale
Registri per lo studio	IN ESSERE attività e accessi penali, esportabili	dall'app, per la durata del contratto

7 Eccezioni e riferimenti normativi

Eccezioni secondo P01 § 8; nessuna eccezione ammette testo dei documenti nei log. Riferimenti: DORA art. 10; Reg. del. (UE) 2024/1774 art. 12; GDPR art. 32; ISO/IEC 27001:2022 controlli 8.15, 8.16, 8.17.

POLITICA P09 · POL-09

Politica di backup e ripristino

Quali copie esistono, dove, per quanto tempo, come si proteggono e come si prova che funzionano. I passi del ripristino sono nella procedura 30.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P09 (POL-09)	Responsabile della sicurezza	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale e dopo ogni prova di ripristino	personale tecnico; uffici ICT risk e continuità operativa dei Clienti	Riservato · per il Cliente

DOCUMENTI COLLEGATI

P04, P12; documento 11 (Continuità operativa, ripristino e incidenti); procedura 30 (Backup e ripristino); procedura 31 (Programma di prova di disaster recovery); documento 12 (Percorso di certificazione e piattaforma)

AMBITO

Il disco dati di ogni ambiente (database, documenti, elaborati, indici, materiali, fatture) e la configurazione necessaria a ricostruire il servizio (infrastruttura come codice, immagini, segreti).

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
8.13, 8.14, 5.30	DORA artt. 11, 12; GDPR art. 32(1)(c)

1 Scopo e ruoli

Le copie servono solo se si ripristinano. Il Responsabile della sicurezza definisce le copie, ne verifica l'esito, guida i ripristini e le prove e firma i verbali; il piano di continuità (documento 11) decide quando ripristinare.

2 Le copie

Tutto lo stato della piattaforma sta su un disco dati cifrato: database, cartelle delle pratiche, materiali, archivi, testi estratti, certificati. Le copie sono queste.

COPIA	FREQUENZA	CONSERVAZIONE	LUOGO
Snapshot giornaliero dell'intero disco	ogni 24 ore alle 02:00 UTC	14 in production (7 staging, 3 development)	Francoforte, cifrato
Copia in Irlanda	di ogni snapshot giornaliero di production	14 giorni	eu-west-1, cifrata
Snapshot prima del rilascio	a ogni rilascio di production, con il commit come etichetta	14 giorni	Francoforte, cifrato
Copia del database prima delle migrazioni	a ogni migrazione	ultime 5	stesso disco: serve a un ritorno rapido, non è una copia di sicurezza

3 Regole

3.1 **Obiettivi.** RPO di 24 ore; RTO di 8 ore per un guasto dell'istanza, del disco o della zona, con ripristino nella stessa regione. Lo snapshot ogni 4 ore (tappa R01), il ripristino regionale in Irlanda con il suo RTO (tappa R03) e gli obiettivi della nuova piattaforma (tappa R14) sono nel Percorso.

3.2 **Cifratura e rotazione.** Ogni copia è cifrata e si conserva 14 giorni; dopo la cancellazione di dati da parte del Titolare, le copie che li contengono escono per rotazione entro 14 giorni.

3.3 **Separazione.** Le copie stanno in due regioni dell'UE. Il volume dei dati si conserva anche se si rimuove lo stack. Le copie protette dalla cancellazione per 7 giorni sono la tappa R11.

3.4 **Ripristino su risorse nuove.** Si ripristina su un volume nuovo, mai sovrascrivendo l'originale, e lo si verifica prima di metterlo in servizio: controllo d'integrità dei database, versione dello schema, conteggio delle righe per tabella, presenza sul disco degli archivi a cui il database rimanda.

3.5 **Ciò che sta fuori dal disco.** Il pool degli utenti, i segreti e le immagini non sono nel disco dati: l'infrastruttura come codice e la procedura 30 dicono come ricostruirli; in un ripristino del pool gli utenti ricevono un nuovo invito e registrano di nuovo l'app di autenticazione.

3.6 **Primo ripiego dell'avvocato.** Il Cliente scarica in ogni momento i propri elaborati; per l'avvocato che deve depositare, l'elaborato già scaricato è il primo ripiego durante un'interruzione.

4 Le prove

1 **A ogni verifica della CI.** Una prova automatica crea una base di dati con lo schema reale, ne fa le copie nei due modi in cui la piattaforma le fa (copia coerente del database e copia dell'intero disco durante una scrittura), le ripristina e verifica integrità, schema, righe e file byte per byte. Se la prova fallisce, il rilascio non parte.

2 **Ogni trimestre, sullo snapshot reale.** L'ultimo snapshot di production si ripristina su un'istanza temporanea isolata, senza porte aperte; si verificano i database e gli archivi, si misurano RPO e RTO; dall'istanza escono solo conteggi e orari, mai contenuti; istanza e volume si cancellano a fine prova.

3 **Verbale.** Ogni prova trimestrale produce un verbale con snapshot usato, RPO e RTO misurati, esito dei controlli e della pulizia; l'esito si comunica al Cliente che lo chiede e sempre ai Clienti DORA.

4 **Prova regionale.** La prova completa di ripristino in Irlanda, annuale, è la tappa R10 del Percorso (procedura 31).

5 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
Snapshot e copia in Irlanda	IN ESSERE 14 snapshot giornalieri e 14 giorni di copie	infrastruttura come codice; elenco degli snapshot
Scadenza delle copie pre-rilascio	IN ESSERE 14 giorni	script di rilascio; elenco degli snapshot
Prova automatica	IN ESSERE a ogni verifica della CI, con il risultato conservato	a ogni pull request e rilascio
Prova trimestrale	IN ESSERE prima prova sullo snapshot di production del [data], RTO misurato [...]	verbale, ogni trimestre

6 Eccezioni e riferimenti normativi

Eccezioni secondo P01 § 8; nessuna eccezione sospende la prova trimestrale per più di un trimestre. Riferimenti: DORA artt. 11 e 12 (ripristino su sistemi separati, par. 3; RTO e RPO coerenti con i livelli di servizio, par. 6); GDPR art. 32, par. 1, lett. c); ISO/IEC 27001:2022 controlli 5.30, 8.13, 8.14.

POLITICA P10 · POL-10

Politica di gestione dei fornitori ICT

Come Trailgun sceglie, contrattualizza, controlla e sostituisce i fornitori che concorrono al servizio, e come ne informa i Clienti.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P10 (POL-10)	Responsabile della sicurezza, con il DPO	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale; registro a ogni cambio di fornitore	uffici outsourcing, ICT risk e DPO dei Clienti	Riservato · per il Cliente

DOCUMENTI COLLEGATI

P02, P11; registro dei subfornitori (15); scheda per il registro delle informazioni (16); procedura 29 (Valutazione dei fornitori); documento 07 (DPA), Allegato 3; documento 18 (Allegato DORA al contratto)

AMBITO

Ogni fornitore che tratta dati dei Clienti, ospita o esegue una parte del servizio o ne condiziona la sicurezza: infrastruttura, modelli, riconoscimento del testo, posta, notifiche, firma, banche dati, pagamenti, codice e CI.

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
5.19-5.23	DORA artt. 28-30; Reg. del. (UE) 2025/532; GDPR artt. 28, 44-46

1 Scopo e ruoli

Il servizio di Trailgun è sicuro quanto la sua catena di fornitura. Il Responsabile della sicurezza valuta e monitora i fornitori e tiene il registro; il DPO valuta i trattamenti di dati personali e i trasferimenti; il legale rappresentante firma i contratti; l'organo amministrativo approva l'ingaggio di un fornitore essenziale.

2 Classi di fornitori

2.1 **Essenziali:** senza di loro il servizio non c'è (Amazon Web Services, che fornisce anche i modelli su Amazon Bedrock).

2.2 **Importanti:** trattano dati dei Clienti per una funzione accessoria (posta, banca dati, firma e visure, notifiche, riconoscimento del testo di riserva).

2.3 **Di supporto:** non ricevono dati dei Clienti (codice e CI, certificati, immagini e pacchetti, posta aziendale salvo la corrispondenza che i Clienti vi mandano).

3 Prima dell'ingaggio

1. **Valutazione** secondo la procedura 29: dati trattati e loro classe (P11), luogo di conservazione e di trattamento, sede del fornitore e della capogruppo, certificazioni (ISO/IEC 27001, SOC 2 di tipo II, C5), conservazione dei dati, uso dei dati per addestramento, subfornitori, solidità, sostituibilità, legge applicabile e accesso di autorità di paesi terzi, disponibilità ad audit, condotta etica. Sono i fattori degli artt. 5 e 6 del Reg. del. (UE) 2024/1773, che Trailgun adotta come modello.
2. **Trasferimenti.** Per un fornitore fuori dall'UE: base del trasferimento, clausole contrattuali tipo (Decisione di esecuzione (UE) 2021/914, modulo 3) e valutazione d'impatto del trasferimento.
3. **Decisione** registrata nel registro 15, con esito, condizioni e data della prossima valutazione. Un fornitore essenziale o importante non si ingaggia senza questa valutazione.
4. **Preavviso ai Clienti** (§ 6) prima che il fornitore riceva dati dei Clienti.

4 Contratto

Con ogni fornitore che tratta dati personali: accordo ex art. 28 GDPR con gli stessi obblighi del DPA di Trailgun verso i Clienti (art. 28, par. 4). Per i fornitori essenziali e importanti, inoltre: misure di sicurezza, notifica degli incidenti, luogo dei dati e preavviso del suo cambio, diritti di audit o rapporti indipendenti, cooperazione con le autorità, restituzione e cancellazione, uscita. Per i servizi che un Cliente DORA usa per una funzione essenziale o importante, Trailgun porta nei subcontratti quanto richiede l'art. 4 del Reg. del. (UE) 2025/532, in particolare gli stessi diritti di accesso e ispezione.

5 Monitoraggio

Il registro dei subfornitori (15) riporta per ciascuno: servizio, classe, dati, luogo, contratto e DPA, garanzie di trasferimento, certificazioni con scadenza, subfornitori rilevanti, data dell'ultima valutazione e della prossima, piano di uscita. Ogni fornitore essenziale e importante si rivaluta ogni anno e dopo un suo incidente rilevante. Il registro dà al Cliente i dati della catena di fornitura che servono al suo registro delle informazioni (Reg. es. (UE) 2024/2956, modelli B_05.01 e B_05.02; scheda 16).

6 Cambi di fornitore e informativa ai Clienti

6.1 L'aggiunta o la sostituzione di un subfornitore che tratta dati dei Clienti si comunica per email all'amministratore e al DPO del Cliente almeno 30 giorni prima, con identità, attività, luogo e garanzie.

6.2 Per i Clienti DORA che usano Trailgun per una funzione essenziale o importante il preavviso è di 60 giorni; il cambiamento non si attua prima della scadenza né finché un'opposizione è pendente (art. 5 del Reg. del. (UE) 2025/532).

6.3 Il Cliente può opporsi entro il periodo di preavviso; se l'opposizione non si risolve in 30 giorni, può recedere senza penali con il rimborso della quota pagata e non goduta.

6.4 Una sostituzione urgente, solo per sicurezza o cessazione del fornitore, si comunica entro 72 ore; il diritto di opposizione resta.

6.5 L'elenco dei subfornitori è allegato al DPA ed è pubblicato, aggiornato, su https://trailgun.ai/subprocessors.

7 Uscita e concentrazione

Per ogni fornitore essenziale e importante Trailgun tiene un piano di uscita: alternativa individuata, dati e configurazioni da trasferire, tempi. L'infrastruttura come codice e i formati aperti dei dati riducono la dipendenza da AWS; la concentrazione resta un rischio accettato e monitorato (politica P02). Nessun ripiego verso un fornitore di modelli fuori dall'UE si attiva: il codice rifiuta qualsiasi regione fuori dall'UE.

8 I fornitori al 01/12/2026

Il dettaglio, con entità contrattuali, garanzie e date di valutazione, è nel registro 15.

FORNITORE E CLASSE	SERVIZIO E DATI	LUOGO	GARANZIE
Amazon Web Services EMEA SARL · essenziale	Infrastruttura, conservazione, login (Cognito), posta di Cognito (SES), Textract, Transcribe, modelli Claude e Titan su Amazon Bedrock; tutti i dati	Germania; copie in Irlanda; modelli in regione UE	DPA; opt-out dal riuso dei contenuti per i servizi di IA di AWS con policy dell'organizzazione; account intestato a Trailgun
Plus Five Five, Inc. (Resend) · importante	Email in uscita e risposte in entrata	Amazon SES in Irlanda; società USA	DPA, clausole contrattuali tipo, valutazione del trasferimento
Wolters Kluwer Italia (One LEGALE) · importante	Banca dati giuridica; riceve solo stringhe di ricerca, senza nomi, codici fiscali, importi o dati delle pratiche (regola in codice con test)	Italia	DPA
Openapi S.p.A., con Namirial · importante	Firma elettronica qualificata e visure camerali	Italia	DPA
Hoss Inc. (DocuPipe) · importante, opzionale	Riconoscimento del testo di riserva, solo per gli studi che lo accendono (spento di default); il singolo file che Textract non legge	USA	DPA, clausole contrattuali tipo, valutazione del trasferimento
Telegram, **Twilio** · per scelta dell'utente	Notifiche su Telegram, SMS e WhatsApp per chi collega quei canali; senza dati delle pratiche	secondo il fornitore	nessun dato delle pratiche nel messaggio
Stripe · per la fatturazione	Carta e addebiti dello studio; nessun dato delle pratiche	UE/USA	condizioni del fornitore
Microsoft	Login per la revisione in Word: il file va dal browser dell'avvocato al tenant del Cliente; non riceve dati da Trailgun	–	–
Google Workspace, **GitHub**, Let's Encrypt, Docker Hub, npm · di supporto	Posta delle persone; codice e CI; certificati; immagini e pacchetti; nessun dato delle pratiche	vari	MFA sulle console; 2FA obbligatoria su GitHub

9 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
DPA con i fornitori	IN ESSERE AWS, Resend, Wolters Kluwer, Openapi, DocuPipe	archivio dei contratti; registro 15
Valutazioni	IN ESSERE prima dell'ingaggio e ogni anno, con le valutazioni dei trasferimenti	procedura 29; registro 15
Elenco pubblicato	IN ESSERE allegato al DPA e pagina pubblica	https://trailgun.ai/subprocessors, a ogni cambio
Preavvisi	IN ESSERE 30 giorni, 60 per i Clienti DORA con funzioni essenziali o importanti	email all'amministratore e al DPO del Cliente

10 Eccezioni e riferimenti normativi

Eccezioni secondo P01 § 8; nessuna eccezione può ammettere un fornitore che tratti dati dei Clienti senza contratto scritto. Riferimenti: DORA artt. 28, 29 e 30; Reg. del. (UE) 2024/1773 e 2025/532; Reg. es. (UE) 2024/2956; GDPR artt. 28 e 44-46; Parere EDPB 22/2024; ISO/IEC 27001:2022 controlli 5.19-5.23.

POLITICA P11 · POL-11

Politica di classificazione e trattamento delle informazioni

Quattro livelli, con le regole di conservazione, trasmissione, condivisione e distruzione di ciascuno.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P11 (POL-11)	Responsabile della sicurezza, con il DPO	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale	tutto il personale e i collaboratori; uffici audit e DPO dei Clienti	Riservato · per il Cliente

DOCUMENTI COLLEGATI
P04, P12, P14, P16; inventario degli asset (42); registro dei trattamenti (40); scheda per il registro delle informazioni (16)

AMBITO
Tutte le informazioni che Trailgun crea, riceve o tratta, in qualsiasi forma: dati dei Clienti sulla piattaforma, documenti interni, codice, corrispondenza.

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
5.12-5.14, 8.11, 8.12	DORA art. 8; Reg. es. (UE) 2024/2956; GDPR artt. 9, 10, 32

1 Scopo e ruoli

La classificazione dice a chiunque lavori per Trailgun come trattare un'informazione senza doverlo chiedere. Il Responsabile della sicurezza assegna il livello agli asset nell'inventario (42); il DPO verifica che i dati personali, e in particolare quelli dell'art. 9 e dell'art. 10 GDPR, siano al livello giusto; ogni persona applica le regole del livello.

2 I livelli

LIVELLO	ESEMPI	REGOLE	SENSIBILITÀ NEL REGISTRO DORA
Pubblico	Sito, materiali commerciali, condizioni pubblicate, elenco dei subfornitori, security.txt	Pubblicazione approvata dal legale rappresentante	–
Interno	Procedure, immagini dei container, metriche di servizio senza dati dei Clienti	Solo personale e fornitori vincolati; nessuna pubblicazione	Low
Riservato	Dati degli utenti e degli studi, fatturazione, contratti, ticket, codice sorgente, i documenti di questo pacchetto	Accesso per necessità; cifratura in transito e a riposo; condivisione solo con chi è vincolato alla riservatezza	Medium
Strettamente riservato	Documenti ed elaborati delle pratiche, conversazioni con gli agenti, dati bancari e creditizi, dati giudiziari, atti penali e intercettazioni, segreti e chiavi, copie di sicurezza	Solo sulla piattaforma o nei servizi AWS indicati nell'inventario; mai su dispositivi personali, email, chat o strumenti non approvati; accesso del personale solo secondo P03 § 4.3, registrato	High

3 Regole

3.1 **Predefinito.** I dati dei Clienti sono «strettamente riservato» per impostazione predefinita, qualunque sia il loro contenuto: Trailgun non li ispeziona per declassarli.

3.2 **Prevalenza.** Il livello più alto prevale: un insieme che contiene un'informazione strettamente riservata è strettamente riservato.

3.3 **Etichetta.** I documenti di Trailgun riportano il livello in copertina o nel piede. I documenti di questo pacchetto sono «Riservato · per il Cliente»; le pagine pubbliche sono pubbliche.

3.4 **Trasmissione.** I dati strettamente riservati escono dalla piattaforma solo per azione dell'utente (download, esportazione, API, comunicazioni ai clienti dello studio che lo studio attiva) o verso i fornitori della politica P10, con i loro contratti. Le notifiche esterne (email, Telegram, SMS, WhatsApp) non portano dati delle pratiche: avvisano e rimandano all'app. Le ricerche sulle banche dati non portano nomi, codici fiscali, importi o dati delle pratiche.

3.5 **Conservazione e distruzione.** Secondo la politica P12. I supporti fisici sono di AWS, che li distrugge secondo le sue procedure attestate.

3.6 **Mascheramento.** Gli agenti lavorano sul testo integrale dei documenti, che è la ragione del servizio: la protezione dei dati delle pratiche è affidata ad accessi, cifratura, regione UE, nessun addestramento e regime rafforzato per il penale (politica P16), non alla pseudonimizzazione.

4 Classificare un'informazione nuova

1 Chi crea o riceve un'informazione nuova (un archivio, un registro, un tipo di file) ne individua il livello con la tabella del § 2; nel dubbio vale il livello più alto.

2 Se è un asset tecnico, il Responsabile della sicurezza lo aggiunge all'inventario (42) con livello, titolare e luogo.

3 Se contiene dati personali, il DPO lo riporta nel registro dei trattamenti (40) e verifica la base e la conservazione.

5 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
Classe degli asset	IN ESSERE livello, titolare e luogo di ogni asset	inventario 42, a ogni cambiamento
Notifiche senza dati delle pratiche	IN ESSERE testo generico con il collegamento all'app	verificabile su ogni canale
Sensibilità per il registro DORA	IN ESSERE corrispondenza con i valori del Reg. es. 2024/2956	scheda 16

6 Eccezioni e riferimenti normativi

Eccezioni secondo P01 § 8; nessuna eccezione declassa dati dei Clienti. Riferimenti: DORA art. 8; Reg. es. (UE) 2024/2956 (sensibilità dei dati, modello B_02.02); GDPR artt. 9, 10 e 32; ISO/IEC 27001:2022 controlli 5.12-5.14, 8.11 e 8.12.

POLITICA P12 · POL-12

Politica di conservazione e cancellazione

Per quanto tempo si tiene ogni dato, come si cancella durante il contratto e alla sua fine, e come si attesta.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P12 (POL-12)	DPO e Responsabile della sicurezza	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale	DPO e uffici audit dei Clienti; personale tecnico	Riservato · per il Cliente

DOCUMENTI COLLEGATI
P09, P11, P16; procedura 28 (Restituzione e cancellazione a fine contratto); certificati 53 (Restituzione dei dati) e 54 (Cancellazione); documento 07 (DPA); documento 56 (Piano di uscita e di transizione)

AMBITO
Tutti i dati della piattaforma, delle copie di sicurezza, dei log e dei fornitori; i dati di cui Trailgun è titolare (utenti, fatturazione).

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
5.33, 8.10	GDPR artt. 5(1)(e), 28(3)(g); DORA art. 30(2)(d); Data Act art. 25

1 Scopo e ruoli

I dati delle pratiche sono dello studio: Trailgun li conserva finché il Titolare li vuole e li cancella quando il Titolare lo chiede o il contratto finisce, in modo completo e verificabile. Il DPO sorveglia termini ed eccezioni di legge; il Responsabile della sicurezza esegue le cancellazioni di fine contratto e firma le attestazioni.

2 Termini di conservazione

DATO	REGOLA
Pratiche, documenti, elaborati, originali	finché il Titolare non cancella la pratica o il cliente; nessuna scadenza automatica durante il contratto
File temporanei di OCR e trascrizione	cancellati a fine analisi; regola di scadenza di 1 giorno sull'archivio temporaneo
Testi estratti e cache OCR	della pratica e dello studio, mai condivisi fra studi; cancellati con la pratica
Conversazioni con gli agenti	cancellate con la pratica, il cliente e lo studio
Indici di ricerca	nella cartella della pratica, cancellati con lei
Documenti scaricati dalla banca dati	compresi nella cancellazione completa dello studio
Eventi di costo	scollegati dai contenuti alla cancellazione; restano gli importi per la fatturazione
Registro delle attività, accessi penali	per la durata del contratto, esportabili; cancellati con lo studio
Log di accesso e applicativi	90 giorni
Log di sicurezza e amministrazione	12 mesi
Copie di sicurezza	14 giorni per ogni copia (giornaliere, pre-rilascio, copie in Irlanda)
Utenti	cancellati con lo studio a fine contratto, anche dal pool di autenticazione
Dati di fatturazione dello studio	10 anni (art. 2220 c.c.); mai dati delle pratiche

3 Durante il contratto

Il Titolare cancella in ogni momento una pratica o un cliente. La cancellazione di una pratica toglie documenti, controlli, versioni, comunicazioni, stati, firme, domande del faldone, attività, notifiche, la cartella dell'atto (originali, testi, indice), la cache OCR della pratica, le conversazioni con gli agenti e i collegamenti dei costi ai contenuti. Le copie di sicurezza che la contenevano escono per rotazione entro 14 giorni.

4 Alla fine del contratto

1. **Accesso in sola lettura per 30 giorni**, con esportazione dall'app.

2. **Esportazione complessiva su richiesta, entro 10 giorni lavorativi**: archivio ZIP cifrato con documenti originali; elaborati in DOCX e PDF/A; testi estratti in TXT; dati strutturati (anagrafiche, risposte dell'assessment, domande e fonti, versioni) in JSON e CSV; registro delle attività e log degli accessi penali in CSV; indice dei file con impronte SHA-256. Consegna tramite link temporaneo cifrato; certificato di restituzione (53). L'esportazione in autonomia dall'app è la tappa R02 del Percorso.
3. **Cancellazione nei 30 giorni successivi** di tutti i dati dello studio, compresi testi estratti, cache OCR, conversazioni con gli agenti, indici, registri delle lavorazioni e utenti, con lo strumento di cancellazione dello studio (procedura 28).
4. **Conferma scritta entro 5 giorni lavorativi** dalla cancellazione: certificato di cancellazione (54).
5. **Copie di sicurezza**: escono per rotazione entro i 14 giorni successivi.
6. **In tutto, al massimo 74 giorni** dalla cessazione (30 + 30 + 14), salvo obblighi di legge. Per i Clienti DORA i termini decorrono dalla fine dell'assistenza all'uscita, che dura fino a 12 mesi (documento 56).

5 Attestazione di cancellazione

Il certificato di cancellazione (54) riporta: Cliente e contratto; data della cessazione e della cancellazione; archivi, cartelle e registri cancellati; utenti rimossi; data entro cui l'ultima copia di sicurezza che conteneva i dati è scaduta; eventuali dati conservati per legge, con la norma e il termine; firma del Responsabile della sicurezza.

6 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
Cancellazione completa della pratica	IN ESSERE cache OCR, conversazioni e collegamenti dei costi compresi, con test	a ogni cancellazione
Strumento di fine contratto	IN ESSERE cancellazione dello studio e dei suoi utenti, anche dal pool	verbale della procedura 28
Rotazione delle copie	IN ESSERE 14 giorni per ogni copia, anche pre-rilascio	elenco degli snapshot
Certificati	IN ESSERE modelli 53 e 54	a ogni cessazione

7 Eccezioni e riferimenti normativi

Eccezioni solo per obbligo di legge o per ordine dell'autorità, documentate e comunicate al Titolare se la legge lo consente. Riferimenti: GDPR artt. 5, par. 1, lett. e), e 28, par. 3, lett. g); DORA art. 30, par. 2, lett. d); Data Act art. 25 (recupero dei dati per almeno 30 giorni e cancellazione completa); art. 2220 c.c.; ISO/IEC 27001:2022 controlli 5.33 e 8.10.

POLITICA P13 · POL-13

Politica di sicurezza del personale e formazione

Prima, durante e dopo il rapporto con chiunque lavori per Trailgun.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P13 (POL-13)	Legale rappresentante	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale	tutto il personale e i collaboratori; uffici audit e HR dei Clienti	Riservato · per il Cliente

DOCUMENTI COLLEGATI
P03, P14, P15; procedura 21 (Ingresso e uscita del personale); registro della formazione (43); revisione degli accessi (44)

AMBITO
Dipendenti, amministratori, soci con ruoli operativi, collaboratori e consulenti con accesso a sistemi o dati di Trailgun o dei Clienti.

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
6.1-6.8	DORA artt. 13(6), 30(2)(i); AI Act art. 4; GDPR artt. 29, 32(4)

1 Scopo e ruoli

Le persone sono il primo controllo e il primo rischio. Il legale rappresentante è titolare di questa politica e firma gli impegni di riservatezza e le designazioni; il Responsabile della sicurezza concede e revoca gli accessi (politica P03) e tiene il registro della formazione (43).

2 Prima del rapporto

2.1 **Verifica dei precedenti** per chi accede alla produzione, nei limiti dell'art. 8 della L. 20 maggio 1970, n. 300 (Statuto dei lavoratori) e dell'art. 10 GDPR, con esito conservato nel fascicolo della persona.

2.2 **Impegno scritto di riservatezza**, che copre il segreto professionale e bancario dei dati dei Clienti e sopravvive alla fine del rapporto, e **designazione al trattamento** con istruzioni scritte (art. 29 GDPR, art. 2-quaterdecies Codice privacy), prima di qualsiasi accesso.

2.3 Nessun accesso prima che i passi 2.1 e 2.2 e la formazione d'ingresso siano completi (procedura 21).

3 Durante il rapporto

3.1 **Formazione su sicurezza e protezione dei dati** all'ingresso e ogni anno, per tutto il personale e i collaboratori con accesso. Contenuti: queste politiche, riconoscimento del phishing, gestione delle credenziali e dell'autenticazione a più fattori, segnalazione degli eventi, regime dei fascicoli penali, risposta agli incidenti.

3.2 **Alfabetizzazione sull'intelligenza artificiale** ogni anno per il personale e, con una sessione di avvio, per gli utenti degli studi: funzionamento e limiti degli agenti, revisione umana, fonti e «N/D», usi esclusi, trasparenza (art. 4 AI Act, obbligo di mezzi).

3.3 Ogni sessione si annota nel registro della formazione (43): persona, ruolo, data, modulo, durata, esito, evidenza.

3.4 Trailgun partecipa, alle condizioni concordate, ai programmi di sensibilizzazione e formazione dei Clienti DORA (art. 13, par. 6, e art. 30, par. 2, lett. i), DORA).

3.5 Le violazioni delle politiche si valutano secondo il contratto e la legge applicabile, con un procedimento che rispetta le garanzie della persona.

4 Alla fine del rapporto

1 Revoca di tutti gli accessi entro 24 ore dalla cessazione (procedura 21).

2 Rotazione dei segreti a cui la persona aveva accesso (procedura 23).

3 Restituzione dei dispositivi o cancellazione verificata dei dati di Trailgun da quelli personali.

4 Promemoria scritto degli obblighi di riservatezza che continuano; verbale di uscita firmato.

5 Chi ha accesso

L'elenco nominativo di chi accede alla produzione, a GitHub, ad AWS, a Google Workspace e ai gruppi amministrativi della piattaforma è nel modello 44 e si rivede ogni trimestre (procedura 22). Alessandro Musella, cofondatore e avvocato, contribuisce al metodo giuridico dei flussi senza accessi alla produzione.

6 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
Riservatezza e designazione	IN ESSERE sottoscritte da chiunque abbia accesso, prima dell'accesso	fascicolo della persona
Verifica dei precedenti	IN ESSERE per chi accede alla produzione	fascicolo della persona
Formazione e alfabetizzazione IA	IN ESSERE prima sessione del `[data]`; poi all'ingresso e ogni anno	registro 43
Uscite	IN ESSERE revoca entro 24 ore, verbale	procedura 21; modello 44

7 Eccezioni e riferimenti normativi

Eccezioni secondo P01 § 8; nessuna eccezione ammette un accesso senza impegno di riservatezza. Riferimenti: DORA artt. 13, par. 6, e 30, par. 2, lett. i); AI Act art. 4; GDPR artt. 29 e 32, par. 4; art. 2-quaterdecies Codice privacy; L. 300/1970 art. 8; ISO/IEC 27001:2022 controlli 6.1-6.8.

POLITICA P14 · POL-14

Politica di uso accettabile

Che cosa possono e non possono fare con sistemi e dati il personale di Trailgun e gli utenti degli studi.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P14 (POL-14)	Responsabile della sicurezza	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale	tutto il personale e i collaboratori; utenti e amministratori degli studi	Riservato · per il Cliente

DOCUMENTI COLLEGATI
P11, P13, P15, P16; inventario degli asset (42); documento 01 (Contratto di servizio); documento 19 (Informativa sull'IA ai clienti dello studio)

AMBITO
Dispositivi, account, posta, strumenti di sviluppo e di IA usati per lavorare per Trailgun; l'uso della piattaforma da parte degli utenti degli studi, insieme alle condizioni del contratto.

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
5.10, 6.7, 8.1	DORA art. 9; L. 132/2025 art. 13; AI Act art. 50

1 Scopo e ruoli

Le regole tecniche funzionano se le persone le rispettano. Il Responsabile della sicurezza fa conoscere questa politica con la formazione (politica P13) e ne verifica il rispetto; ogni persona ne risponde. Per gli utenti degli studi le regole valgono insieme al contratto di servizio.

2 Personale di Trailgun

- Dispositivi con disco cifrato, blocco automatico dello schermo e sistema aggiornato, registrati nell'inventario degli asset (42); autenticazione a più fattori su ogni account di lavoro.
- I dati dei Clienti si consultano solo sulla piattaforma o nei sistemi di AWS, e solo nei casi della politica P03 § 4.3; non si scaricano su dispositivi, non si inviano per email o chat, non si copiano in altri ambienti.
- Nessun dato dei Clienti, documento delle pratiche o segreto in strumenti di IA, traduttori o servizi web non approvati, compresi gli assistenti di programmazione.
- Vietato condividere credenziali, disattivare o aggirare un controllo, fare prove di sicurezza su production senza autorizzazione scritta, usare la piattaforma per scopi personali.
- Lavoro da remoto: reti fidate o VPN, nessuna sessione aperta su dispositivi altrui, attenzione a chi vede lo schermo.
- Ogni evento sospetto (email anomala, dispositivo perso, accesso inatteso) si segnala subito a security@trailgun.ai.
- L'uso dei sistemi aziendali può essere verificato nei limiti della L. 300/1970 e del GDPR, con informativa preventiva.

3 Utenti degli studi

- Ogni elaborato è una bozza che il professionista rivede prima di usarla; ogni segnalazione è una segnalazione con fonte, non una conclusione. La pagina dell'atto lo ricorda e i file prodotti dagli agenti portano la marcatura di contenuto generato con IA (politica P15).
- Le chat con l'assistente dell'atto e con l'assistenza dicono all'utente che sta parlando con un agente di IA; le mail che lo studio fa inviare in modalità automatica (richieste ai clienti, trattative) dicono ai destinatari che le ha preparate e inviate un agente di IA per conto dello studio.
- Si caricano solo i documenti necessari alla pratica; categorie particolari di dati solo nella misura necessaria.
- Credenziali e dispositivo di autenticazione sono personali; un dispositivo perso si segnala all'amministratore dello studio.
- L'avvocato informa i propri clienti dell'uso dell'IA (art. 13, c. 2, L. 132/2025); Trailgun fornisce il testo (documento 19).
- Non è consentito usare Trailgun per finalità escluse: uso da parte di un'autorità giudiziaria o per suo conto, valutazione del merito creditizio di persone fisiche, valutazione dell'affidabilità delle prove per conto di autorità di contrasto, profilazione di persone (politica P15).
- Per i fascicoli penali, la materia «penale» si sceglie nel modulo prima di caricare l'archivio, e nel titolo della pratica non si scrivono nomi di indagati o imputati (politica P16).

4 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
Presa visione del personale	IN ESSERE firmata con l'impegno di riservatezza	fascicolo della persona; formazione annuale (43)
Dispositivi	IN ESSERE cifratura, blocco, aggiornamenti	inventario 42; revisione trimestrale (44)
Avvisi di IA agli utenti e ai destinatari	IN ESSERE chat, pagina dell'atto, mail automatiche	verificabili nell'app

5 Eccezioni e riferimenti normativi

Eccezioni secondo P01 § 8. Riferimenti: DORA art. 9; L. 132/2025 art. 13 (uso dell'IA nelle professioni intellettuali: attività strumentali e di supporto, prevalenza del lavoro intellettuale, informazione al cliente); AI Act art. 50, par. 1; L. 300/1970; ISO/IEC 27001:2022 controlli 5.10, 6.7, 8.1.

POLITICA P15 · POL-15

Politica di governance dell'intelligenza artificiale

Ruoli, usi ammessi ed esclusi, modelli, dati, trasparenza, sorveglianza umana e gestione dei cambiamenti dell'IA di Trailgun.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P15 (POL-15)	Responsabile della conformità IA, [nome]	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale e a ogni cambio di modello, di fornitore o di finalità	personale; uffici compliance e DPO dei Clienti; studi	Riservato · per il Cliente

DOCUMENTI COLLEGATI

documento 09 (AI Act e uso dell'IA nella professione), con le schede dei modelli; P05, P13, P14, P16; documento 19 (Informativa sull'IA ai clienti dello studio); documento 47 (Mappa AI Act → controlli); documento 60 (Dichiarazione: nessun addestramento sui dati dei clienti)

AMBITO

Il sistema di IA Trailgun: gli agenti dei verticali, dell'analisi del faldone, della ricerca fonti, dell'assistente dell'atto e dell'assistenza; i classificatori; gli embeddings; i servizi di riconoscimento del testo e della voce.

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
5.1, 5.31, 5.34; ISO/IEC 42001 come riferimento	AI Act artt. 4, 5, 6, 25, 50, 53; L. 132/2025 art. 13; GDPR art. 22

1 Ruoli secondo l'AI Act

Trailgun è fornitore del sistema di IA Trailgun (art. 3, punto 3, Reg. (UE) 2024/1689) e fornitore a valle rispetto al modello per finalità generali che integra (art. 3, punto 68). Il fornitore del modello Claude ai sensi dell'AI Act è Anthropic, firmataria del codice di buone pratiche per i modelli per finalità generali; il servizio che esegue il modello è Amazon Bedrock di AWS, nell'UE, e Anthropic non riceve i dati dei Clienti. Studi, banche e servicer sono deployer (art. 3, punto 4).

2 Ruoli in Trailgun

2.1 **Legale rappresentante**, Franco Puppo, CEO: approva la classificazione, i cambi di modello o di fornitore del modello e le nuove finalità.

2.2 **Responsabile della conformità IA**, [nome]: titolare di questa politica; tiene il memorandum di classificazione, il fascicolo tecnico e il registro degli eventi dell'IA; istruisce le revisioni.

2.3 **Responsabile della sicurezza**: sicurezza dei modelli e dei dati (politiche P01–P12). **DPO**: trattamenti e valutazioni d'impatto. **Alessandro Musella**, avvocato e cofondatore: metodo giuridico e legal design dei flussi, senza ruoli esecutivi.

3 Finalità e classificazione

3.1 **Finalità prevista:** assistere avvocati, banche e servicer nell'analisi dei documenti delle pratiche e nella preparazione di bozze di atti, relazioni e risposte, che il professionista rivede.

3.2 **Non ad alto rischio.** L'Allegato III, punto 8, lett. a), riguarda i sistemi usati da un'autorità giudiziaria o per suo conto (considerando 61): non l'avvocato di parte, il servicer o la banca. La due diligence sui crediti valuta documenti e garanzie, non il merito creditizio di persone fisiche (punto 5, lett. b). La valutazione è documentata nel memorandum di classificazione (documento 09).

3.3 **Usi esclusi**, scritti nel contratto, nella documentazione e nei materiali commerciali: vendita o uso per uffici giudiziari o per loro conto, compresi gli ausiliari del giudice che lo usino in quella veste; valutazione del merito creditizio o punteggio di persone fisiche; valutazione dell'affidabilità delle prove per autorità di contrasto; profilazione di persone fisiche; valutazione del rischio che una persona commetta un reato (art. 5, par. 1, lett. d). Trailgun dichiara che il sistema non è destinato a diventare un sistema ad alto rischio (art. 25, par. 2).

3.4 Una nuova finalità, un nuovo verticale o un nuovo cliente che ne cambi l'uso si valutano prima della vendita e si documentano. Se l'uso cambiasse verso l'Allegato III, gli obblighi dell'alto rischio si applicherebbero dal 02/12/2027.

4 Inventario dei componenti di IA

COMPONENTE	USO	MODELLO E LUOGO
Agenti (46)	Lettura, raccolta dati, redazione, controllo, domande, ricerca fonti, assistente dell'atto, assistenza	Claude su Amazon Bedrock, in una regione dell'UE; modello predefinito Claude Opus 5.5, assegnato solo dalla piattaforma; richieste firmate dal ruolo dell'istanza
Classificatori	Natura del fascicolo, analisi per documento	come gli agenti
Embeddings	Ricerca «veloce» dell'analisi del faldone; mai sul penale	Amazon Titan Text Embeddings V2 su Bedrock, nell'UE; senza, ricerca solo lessicale (BM25)
Riconoscimento del testo	OCR con coordinate	Amazon Textract, Francoforte; riserva DocuPipe solo per gli studi che la accendono
Trascrizione	Audio del faldone, parlanti distinti	Amazon Transcribe, Francoforte

5 Dati

5.1 **Nessun addestramento** sui dati dei Clienti, né da Trailgun né dai fornitori dei modelli: i modelli su Amazon Bedrock non conservano né usano i prompt per addestrare, e il riuso dei contenuti per il miglioramento dei servizi di IA di AWS (Textract, Transcribe, Bedrock) è escluso con una policy dell'organizzazione AWS di Trailgun (documento 60).

5.2 **Solo nell'UE.** Il codice rifiuta qualsiasi regione fuori dall'UE per i modelli e per gli embeddings, prima che un dato lasci il server.

5.3 **Prompt.** Stanno nel registro dei prompt; il loro testo si legge e si cambia solo dal backoffice della piattaforma e non esce verso il browser di uno studio. Lo studio vede di ogni prompt una sintesi e può solo aggiungere testi propri, accodati.

5.4 **Memoria dello studio.** Le regole confermate dall'avvocato si scrivono solo nei testi aggiuntivi dello studio, mai nel testo di Trailgun; gli elaborati di un Cliente non servono a produrre elaborati per altri.

6 Qualità, trasparenza e sorveglianza umana

6.1 **Fonti.** Ogni dato di un elaborato viene dai documenti, con la fonte, o è «N/D»; i riferimenti a documento e pagina dell'analisi del faldone si verificano in codice prima di mostrarli.

6.2 **Revisione umana.** Ogni elaborato è rivisto dal professionista prima dell'uso; nessuna decisione basata unicamente su un trattamento automatizzato (art. 22 GDPR). La pagina dell'atto lo ricorda.

6.3 **Interazione (art. 50, par. 1).** L'utente sa di parlare con un agente di IA: avviso nell'assistente dell'atto e nella chat dell'assistenza. Le mail inviate in modalità automatica (richieste ai clienti dello studio, trattative) dicono ai destinatari che le ha preparate e inviate un agente di IA per conto dello studio.

6.4 **Marcatura (art. 50, par. 2).** I file DOCX e PDF prodotti dagli agenti, compreso il PDF della revisione in Word, portano nei metadati una marcatura leggibile da macchina («AI-generated, EU AI Act art. 50») e il tipo di fonte digitale IPTC per i contenuti generati da un modello. Le copie dei documenti del Cliente e le fatture non si marcano mai.

6.5 **Informazione ai clienti dell'avvocato.** Trailgun fornisce agli avvocati il testo con cui informare i propri clienti dell'uso dell'IA, obbligo dell'avvocato ai sensi dell'art. 13, c. 2, L. 132/2025 (documento 19).

6.6 **Alfabetizzazione** del personale e degli utenti secondo la politica P13 (art. 4).

7 Cambiamenti

1 **Revisione di classificazione** prima di ogni nuovo verticale, funzione, modello o fornitore del modello, e ogni anno.

2 **Prova comparativa** documentata su pratiche di prova senza dati dei Clienti prima di cambiare il modello predefinito di un agente.

3 **Approvazione** del legale rappresentante e annotazione nel registro dei cambiamenti (45).

4 **Preavviso** agli studi secondo la politica P10 se cambia il fornitore che esegue i modelli; aggiornamento delle schede dei modelli (documento 09).

8 Eventi e incidenti dell'IA

Un comportamento del sistema che può portare un professionista a usare un elaborato sbagliato senza accorgersene, o che espone dati, è un evento dell'IA: per esempio una citazione segnata come verificata che nel documento non c'è, dati di un'altra pratica in un elaborato, errori sistematici su importi o termini, un'istruzione nascosta in un documento che altera un agente. Si segnala a security@trailgun.ai o dall'assistenza, si spegne la funzione interessata (ogni passo è un'opzione), si avvisano gli studi coinvolti con le pratiche da ricontrollare, se ne cerca la causa e si registra; se tocca più studi o i dati, è un incidente (procedura 25).

9 Documenti tenuti e percorso

Memorandum di classificazione e schede dei modelli (documento 09), fascicolo tecnico (documentazione del fornitore del modello ai sensi dell'art. 53, schede, prove comparative), registro degli eventi dell'IA, registro della formazione (43), registro dei fornitori (15). La valutazione ISO/IEC 42001 è un obiettivo del Percorso (tappa R17), costruito sopra il sistema di gestione della sicurezza.

10 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
Modelli e embeddings nell'UE	IN ESSERE Bedrock in regione UE; controllo della regione nel codice, con test	configurazione di production; verifica della CI
Nessun addestramento	IN ESSERE condizioni di Bedrock; policy di opt-out dell'organizzazione AWS	documento 60
Marcatura e avvisi	IN ESSERE metadati in DOCX e PDF; avvisi in chat, sulla pagina dell'atto e nelle mail automatiche	verificabili su ogni file prodotto
Classificazione	IN ESSERE memorandum e usi esclusi	documento 09; revisione annuale

11 Eccezioni e riferimenti normativi

Nessuna eccezione agli usi esclusi del § 3.3. Riferimenti: Reg. (UE) 2024/1689 artt. 3, 4, 5, 6, 25, 50, 53 e Allegato III, come modificati dal Reg. (UE) 2026/1744; L. 132/2025 art. 13; GDPR artt. 22 e 35; Parere EDPB 28/2024; ISO/IEC 42001:2023 come riferimento.

POLITICA P16 · POL-16

Politica sui fascicoli penali: regime rafforzato

Le regole in più per i fascicoli penali e misti: atti di indagine, intercettazioni e loro trascrizioni, dati relativi a reati.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P16 (POL-16)	DPO e Responsabile della sicurezza	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale	studi che trattano fascicoli penali; loro DPO; personale di Trailgun	Riservato · per il Cliente

DOCUMENTI COLLEGATI

P02, P03, P08, P11, P12, P15; documento 09 (AI Act e uso dell'IA nella professione); documento 50 (Supporto alla DPIA del Titolare); procedure 25 (Risposta agli incidenti) e 26 (Violazioni dei dati personali)

AMBITO

Ogni analisi del faldone per la quale l'avvocato ha scelto la materia «penale» nel modulo o che il classificatore della natura riconosce come penale o mista, con i suoi documenti, audio, trascrizioni, elaborati, domande e funzioni (matrice, timeline, grafo, scheda dell'imputato, iter delle intercettazioni).

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
5.12, 5.34, 8.3, 8.15	GDPR artt. 10, 35; art. 2-octies Codice privacy; artt. 114, 268, 269 c.p.p.

1 Perché un regime a sé

I fascicoli penali contengono dati relativi a reati (art. 10 GDPR), trattabili dall'avvocato per la difesa (art. 2-octies, c. 3, lett. e), Codice privacy), spesso voci e conversazioni di terzi, e atti la cui diffusione è vietata o limitata dalla disciplina processuale (in particolare artt. 114, 268 e 269 c.p.p.). Una loro esposizione ha impatto «molto alto» per definizione (politica P02) e nessun rischio sulla loro riservatezza si accetta oltre il livello medio.

2 Ruoli

Il DPO sorveglia l'applicazione di questa politica e approva, con istruzione scritta del Titolare, ogni eccezione; il Responsabile della sicurezza ne cura i controlli tecnici e il registro degli accessi del personale. L'avvocato dichiara la materia e decide che cosa caricare.

3 Regole

3.1 **Dichiarazione della materia.** L'avvocato sceglie la materia «penale» nel modulo prima di caricare l'archivio. Se non la sceglie, il fascicolo è trattato come penale quando il classificatore della natura lo riconosce penale o misto; la scelta esplicita fa valere il regime fin dal primo passo.

3.2 **Niente embeddings.** Sui fascicoli penali o misti non si costruisce l'indice semantico: la ricerca è solo per parole, anche per gli indici costruiti alla prima domanda.

3.3 **Registro degli accessi.** Ogni consultazione dei risultati (una all'ora per utente), domanda, analisi, confronto fra depositi, timeline, grafo e scheda dell'imputato generati diventa una riga del registro delle attività dello studio, con chi, quando e che cosa; il Titolare lo esporta. La scrittura del registro non blocca l'operazione se fallisce: l'errore va nei log.

3.4 **Modelli solo nell'UE.** Il testo dei fascicoli penali, come ogni altro testo, si elabora solo con Claude su Amazon Bedrock in una regione dell'UE; il fornitore del modello non riceve i dati e nessuno li usa per addestrare (politica P15).

3.5 **Audio e intercettazioni.** La trascrizione si fa con Amazon Transcribe a Francoforte, tramite un archivio temporaneo cifrato che scade entro 1 giorno; il riuso dei contenuti per i servizi di IA di AWS è escluso con una policy dell'organizzazione AWS di Trailgun.

3.6 **Nessun servizio fuori dall'UE.** Lo studio che tratta fascicoli penali lascia spento l'OCR di riserva negli Stati Uniti (DocuPipe, spento di default); le notifiche esterne non portano dati delle pratiche; le ricerche su One LEGALE non portano nomi, codici fiscali, importi o dati delle pratiche, per una regola in codice con test.

3.7 **Personale.** Nessun accesso del personale al contenuto se non su richiesta scritta dello studio o per un incidente, annotato nel registro degli accessi del personale. Il backoffice mostra i titoli delle pratiche: nel titolo lo studio non scrive nomi di indagati o imputati (politica P14).

3.8 **Segnalazioni, non conclusioni.** Le funzioni sul fascicolo (matrice, contraddizioni, filtro e scheda dell'imputato, iter delle intercettazioni) riportano ciò che gli atti dicono, con la fonte; non valutano la colpevolezza né il rischio che una persona commetta un reato.

3.9 **Cancellazione.** Alla cancellazione della pratica non resta nulla del fascicolo: documenti, audio, trascrizioni, testi, cache OCR, conversazioni con gli agenti e indici; le copie di sicurezza escono per rotazione entro 14 giorni (politica P12).

3.10 **Incidenti.** Un incidente che può toccare la riservatezza di un fascicolo penale si classifica «grave» (procedura 25) e si notifica al Titolare entro le 24 ore previste per le violazioni, senza attendere la certezza (procedura 26).

3.11 **DPIA.** Trailgun fornisce allo studio entro 10 giorni lavorativi le informazioni per la valutazione d'impatto, che il trattamento su larga scala di dati relativi a reati richiede (art. 35, par. 3, lett. b), GDPR), con il modello del documento 50.

4 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
Materia, niente embeddings, registro degli accessi	IN ESSERE regole in codice, con test	registro esportabile dallo studio
Modelli nell'UE; nessun servizio fuori dall'UE	IN ESSERE Bedrock in regione UE; DocuPipe spento di default; notifiche e ricerche senza dati	configurazione di production; registro 15
Cancellazione completa	IN ESSERE cache OCR e conversazioni comprese	a ogni cancellazione
Registro degli accessi del personale	IN ESSERE ogni accesso con richiesta e motivo	estratto al Titolare su richiesta

5 Eccezioni e riferimenti normativi

Nessuna eccezione alle regole 3.2-3.7 senza istruzione scritta del Titolare e parere del DPO. Riferimenti: GDPR artt. 10, 25, 32 e 35; art. 2-octies Codice privacy; artt. 114, 268 e 269 c.p.p.; AI Act art. 5, par. 1, lett. d); norme del Codice deontologico forense sul segreto e sulla riservatezza.

POLITICA P17 · POL-17

Politica di gestione delle segnalazioni (whistleblowing)

Il canale per segnalare violazioni di legge o delle politiche, con la tutela di chi segnala.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P17 (POL-17)	Gestore delle segnalazioni, [persona o soggetto esterno]	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026
REVISIONE	DESTINATARI		CLASSIFICAZIONE
annuale	personale, collaboratori, fornitori, soci, candidati ed ex collaboratori; uffici compliance dei Clienti		Riservato · per il Cliente

DOCUMENTI COLLEGATI
P01, P07, P13; procedura 24 (Gestione delle vulnerabilità e segnalazione responsabile); procedura 25 (Risposta agli incidenti)

AMBITO
Personale, collaboratori, consulenti, fornitori e loro dipendenti, soci, candidati ed ex collaboratori di Trailgun che vengono a conoscenza di violazioni nel contesto lavorativo.

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
6.8	D.Lgs. 10 marzo 2023, n. 24; direttiva (UE) 2019/1937; GDPR

1 Scopo e inquadramento

Il D.Lgs. 10 marzo 2023, n. 24, attua la direttiva (UE) 2019/1937 sulla protezione delle persone che segnalano violazioni. Trailgun ha valutato la propria posizione rispetto al decreto ([esito della valutazione e data]) e in ogni caso adotta un canale interno con le garanzie del decreto, perché i Clienti finanziari lo chiedono ai fornitori e perché chi vede un problema deve poterlo dire senza timore.

2 Che cosa si può segnalare

Violazioni di legge o di regolamento, delle politiche di Trailgun e del contratto con i Clienti di cui la persona viene a conoscenza nel contesto lavorativo: per esempio un uso dei dati dei Clienti fuori dalle istruzioni, un controllo di sicurezza aggirato, un'informazione falsa data a un Cliente o a un'autorità. Le vulnerabilità tecniche trovate da ricercatori esterni seguono la segnalazione responsabile della procedura 24.

3 Ruoli

Il gestore delle segnalazioni, [persona o soggetto esterno], autonomo e formato, riceve e gestisce le segnalazioni; il sostituto, [soggetto esterno], le gestisce quando la segnalazione riguarda il gestore o il legale rappresentante. L'organo amministrativo riceve ogni anno un resoconto anonimo del numero e dell'esito delle segnalazioni.

4 Come si gestisce una segnalazione

1. **Canale.** Segnalazioni scritte, anche anonime, tramite [piattaforma cifrata o casella dedicata], e orali su richiesta, con incontro entro un termine ragionevole. Il canale è separato dalla posta ordinaria e accessibile solo al gestore. Le istruzioni sono pubblicate su [pagina del sito].
2. **Avviso di ricevimento** entro 7 giorni dalla ricezione.
3. **Istruttoria.** Il gestore valuta l'ammissibilità, chiede se serve chiarimenti a chi segnala, raccoglie i riscontri con la riservatezza del § 5.
4. **Riscontro** a chi segnala entro 3 mesi dall'avviso di ricevimento (art. 5 D.Lgs. 24/2023).
5. **Eventi di sicurezza.** Una segnalazione che descrive un incidente o una vulnerabilità si passa subito, con la riservatezza dell'identità, al Responsabile della sicurezza (procedura 25).

5 Tutele

5.1 **Riservatezza.** L'identità di chi segnala e delle persone coinvolte non si rivela senza consenso, salvo i casi di legge (art. 12).

5.2 **Divieto di ritorsione** verso chi segnala in buona fede e verso chi lo assiste (art. 17).

5.3 **Canale esterno.** Chi segnala è informato della possibilità di rivolgersi all'ANAC alle condizioni di legge.

5.4 **Dati personali.** Le segnalazioni si trattano con l'informativa ai segnalanti e si conservano per il tempo necessario alla gestione e comunque non oltre i termini di legge.

6 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
Canale e gestore	IN ESSERE [strumento]; gestore e sostituto nominati	atto di nomina; istruzioni pubblicate
Registro delle segnalazioni	IN ESSERE data, avviso, riscontro, esito; accessibile solo al gestore	a ogni segnalazione
Resoconto annuale	IN ESSERE numero ed esito, in forma anonima	all'organo amministrativo, ogni anno

7 Eccezioni e riferimenti normativi

Nessuna eccezione alla riservatezza dell'identità e al divieto di ritorsione. Riferimenti: D.Lgs. 10 marzo 2023, n. 24 (in particolare artt. 4, 5, 12 e 17); direttiva (UE) 2019/1937; GDPR; ISO/IEC 27001:2022 controllo 6.8.

ALLEGATO A

Registro dei rischi ICT in sintesi

Le famiglie di rischio del registro, con i controlli principali in essere e le tappe del Percorso che le riducono ancora. Il registro completo, con probabilità, impatto, rischio inerente e residuo, titolare, trattamento e data di riesame di ogni voce, è il foglio 41 (Registro dei rischi ICT), costruito con il metodo della politica P02 e consegnato ai Clienti DORA che lo chiedono.

FAMIGLIA	SCENARIO TIPICO	CONTROLLI PRINCIPALI IN ESSERE	PERCORSO
Disponibilità della piattaforma	Guasto dell'istanza, del disco o della zona; perdita della regione di Francoforte	Snapshot giornalieri e copie cifrate in Irlanda; infrastruttura come codice; sonda ogni minuto e allarmi 24/7; prova di ripristino trimestrale con RTO misurato; procedure 30 e 31	R01, R03, R10, R12, R14
Perdita o cancellazione malevola dei dati	Corruzione, errore umano, ransomware anche sulle copie	Copie cifrate in due regioni dell'UE; volume conservato alla rimozione dello stack; nessuna porta SSH; GuardDuty; credenziali temporanee	R11, R12
Accesso non autorizzato	Furto o abuso di credenziali degli utenti o del personale	TOTP obbligatorio per gli utenti; MFA su ogni console; IAM Identity Center; CloudTrail 12 mesi; sessioni registrate; revisione trimestrale degli accessi	–
Isolamento fra studi	Un errore logico espone dati di uno studio a un altro	Predicato unico di visibilità con test; ruoli applicati lato server; verifica obbligatoria a ogni rilascio	R06
Attacco all'applicazione e catena del software	Vulnerabilità in dipendenze, immagini o proxy; segreti esposti	HSTS e intestazioni di sicurezza; container non root; proxy a versione fissata; Dependabot; scansione delle immagini; gitleaks; tempi di correzione di P07	R05, R06, R12
Luogo dei dati e trasferimenti	Dati delle pratiche fuori dall'UE o riusati da un fornitore	Modelli ed embeddings su Bedrock nell'UE, con controllo della regione in codice; opt-out dei servizi di IA di AWS; DocuPipe solo per scelta dello studio; notifiche e ricerche senza dati delle pratiche	–
Fornitori e concentrazione	Dipendenza da AWS per infrastruttura e modelli; guasto di un fornitore	Catena corta e contrattualizzata (P10); valutazione annuale; piani di uscita; formati aperti dei dati	R09
Errori dell'IA	Dato inventato, citazione errata, istruzioni nascoste in un documento	Fonte o «N/D» per ogni dato; riferimenti verificati in codice; revisione del professionista; marcatura e avvisi art. 50; formazione	R06
Conservazione e cancellazione	Dati che sopravvivono alla cancellazione o al contratto	Cancellazione completa della pratica e dello studio; copie a 14 giorni; certificati 53 e 54	R02
Notifica ai Clienti DORA	Incidente comunicato in ritardo	security@trailgun.ai presidiata; reperibilità 24/7 per la priorità 1; allarmi; procedura 25 a tre livelli; modelli 51	R04
Fascicoli penali	Esposizione di atti di indagine o intercettazioni	Regime rafforzato di P16: niente embeddings, registro degli accessi, nessun servizio fuori dall'UE, cancellazione completa	–
Persona chiave e separazione dei compiti	Squadra tecnica piccola: assenza di chi gestisce rilasci e ripristini	Procedure scritte; branch protetti con verifica obbligatoria; identità personali; registri di amministrazione	R09, R13
Conformità e posizione contrattuale	Requisito del Cliente o dell'autorità non soddisfatto	Politiche approvate; DPO nominato; DPA con i fornitori; polizze cyber e RC professionale; pacchetto di conformità	R07, R08, R15, R16

ALLEGATO B

Mappa delle corrispondenze

Dove trovare, nel pacchetto di conformità, la risposta a ciascun requisito che il Cliente porta al fornitore. I numeri sono quelli dei documenti del pacchetto; le mappe complete per DORA, GDPR, AI Act e linee guida EBA sono i fogli 17, 46, 47 e 48.

REQUISITO	FONTE	DOVE
Politica di sicurezza delle informazioni	DORA art. 9, par. 4, lett. a)	P01
Quadro di gestione del rischio, inventari, dipendenze	DORA artt. 6, 8; art. 16, par. 1, lett. e)	P02; fogli 41, 42; P10 § 8; registro 15

REQUISITO	FONTE	DOVE
Accessi limitati e autenticazione forte	DORA art. 9, par. 4, lett. c)-d); Reg. del. 2024/1774 artt. 19-21	P03; procedure 21, 22; modello 44
Cifratura secondo la classificazione	DORA art. 9, par. 4, lett. d); Reg. del. 2024/1774 art. 6	P04, P11; procedura 23
Gestione dei cambiamenti TIC	DORA art. 9, par. 4, lett. e)	P05; procedura 20; registro 45
Patch e vulnerabilità	DORA art. 9, par. 4, lett. f); Reg. del. 2024/1774 art. 10	P07; procedura 24
Test del software del fornitore	Reg. del. 2024/1774 art. 16	P06
Rilevazione delle anomalie e log	DORA art. 10; Reg. del. 2024/1774 art. 12	P08
Continuità, BIA, piani testati	DORA art. 11; Reg. del. 2024/1774 art. 25	documento 11; procedura 31
Backup, ripristino su sistemi separati, RTO e RPO	DORA art. 12	P09; procedure 30, 31
Riesame post-incidente e formazione	DORA art. 13, par. 2 e 6	procedura 25; P13; registro 43
Comunicazione di crisi	DORA art. 14	documento 11
Incidenti: classificazione e dati per le segnalazioni	DORA artt. 17-19; Reg. 2024/1772, 2025/301, 2025/302	procedura 25; modelli 51
Test di resilienza, partecipazione al TLPT	DORA artt. 24-26; art. 30, par. 3, lett. d)	P07 § 5; procedura 31; documento 12
Luogo dei dati e preavviso di cambio	DORA art. 30, par. 2, lett. b)	P10 §§ 6 e 8; documento 61
Restituzione dei dati e uscita	DORA artt. 28, par. 8, e 30, par. 2, lett. d), par. 3, lett. f); Data Act art. 25	P12 § 4; procedura 28; documento 56
Assistenza negli incidenti senza costi	DORA art. 30, par. 2, lett. f)	documento 11; procedura 25
Cooperazione con le autorità, ispezioni	DORA art. 30, par. 2, lett. g), par. 3, lett. e); D.Lgs. 23/2025 art. 8	P01 § 6; documento 18
Subappalto di funzioni essenziali o importanti	Reg. del. 2025/532 artt. 3-6	P10 §§ 4 e 6
Sicurezza del trattamento	GDPR art. 32	P03, P04, P08, P09
Violazioni dei dati personali	GDPR art. 33, par. 2	procedura 26
Cancellazione o restituzione a fine servizio	GDPR art. 28, par. 3, lett. g)	P12; certificati 53, 54
Dati relativi a reati, DPIA	GDPR artt. 10 e 35; art. 2-octies Codice privacy	P16; documento 50
Alfabetizzazione, trasparenza, catena del valore dell'IA	AI Act artt. 4, 25, 50	P13, P15; documento 09
Personale e uso dei sistemi	DORA art. 30, par. 2, lett. i)	P13, P14; procedura 21
Segnalazioni delle violazioni	D.Lgs. 24/2023	P17

Trailgun

On target.

In a flash.

Dai documenti al lavoro finito: agenti AI per pratiche legali e finanziarie.

SICUREZZA E INCIDENTI
security@trailgun.ai

PRIVACY E DPO
privacy@trailgun.ai

REPERIBILITÀ PRIORITÀ 1
[+39 ...]

[Trailgun S.r.l.] · sede [indirizzo] · P.IVA [...] · LEI [...]. Le diciassette politiche sono anche documenti separati del pacchetto di conformità (P01-P17). Documento riservato, destinato al Cliente e alle sue autorità di vigilanza.