Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO 05



VERSIONE 2.0 · DICEMBRE 2026

Sicurezza delle informazioni

Governance, architettura, accessi, cifratura, sviluppo, vulnerabilità, log, backup, continuità, incidenti, fornitori, fascicoli penali e intelligenza artificiale. Ogni misura descritta è in essere alla data del documento e ha un'evidenza che si mostra in audit.

DESTINATARI
Banche, intermediari 106, servicer, studi

RIFERIMENTI
DORA · GDPR art. 32 · ISO/IEC 27001

CLASSIFICAZIONE
Riservato

COME LEGGERE QUESTO DOCUMENTO

Uno stato solo: in essere, con l'evidenza

Ogni affermazione sulla piattaforma corrisponde al codice in produzione e alla configurazione AWS di Trailgun al 01/12/2026. I numeri (livelli di servizio, RPO, RTO, tempi di notifica, conservazione) sono gli stessi in tutti i documenti del pacchetto di conformità. Le tappe successive (certificazione, nuova piattaforma) hanno un codice R e una data nel documento 12, Percorso di certificazione e piattaforma.

IN ESSERE

Attivo in produzione, con un'evidenza (configurazione, codice, test, verbale o registro) che si mostra in sede di audit.

PERCORSO R01-R17

Tappa del Percorso di certificazione e piattaforma: qui solo il codice, la data e l'evidenza attesa nel documento 12.

QUADRO

1 Scopo, ambito e destinatari
2 Governance, ruoli e responsabilità
3 SGSI e percorso ISO/IEC 27001

ARCHITETTURA E DATI

4 Architettura
5 Flussi dei dati per canale
6 Isolamento tra studi

CONTROLLI TECNICI

7 Identità e accessi
8 Cifratura e chiavi
9 Sicurezza della rete
10 Sviluppo sicuro e cambiamenti
11 Vulnerabilità e patch
12 Log e monitoraggio

RESILIENZA

13 Backup e ripristino
14 Continuità operativa
15 Gestione degli incidenti

PERSONE, LUOGHI, FORNITORI

16 Sicurezza fisica
17 Personale e formazione
18 Fornitori e catena di fornitura

REGIMI SPECIALI E VERIFICHE

19 Fascicoli penali
20 Sicurezza dell'intelligenza artificiale
21 Test, verifiche e audit
22 Certificazioni, assicurazioni e percorso

A-C Allegati
EN English summary · pagina 4

Controllo del documento

VOCE	VALORE
Versione e data	2.0 · stato al 01/12/2026
Redatto e approvato	Franco Puppo, CEO, responsabile della sicurezza; approvato dall'organo amministrativo il [data]
Aggiornamento	Dopo ogni cambiamento rilevante o incidente grave, a ogni tappa del Percorso e almeno una volta l'anno
Distribuzione	Riservata: clienti e potenziali clienti, per la valutazione del fornitore, sotto obbligo di riservatezza

IN SINTESI

Una piattaforma piccola, tutta nell'Unione

Trailgun è un servizio SaaS su Amazon Web Services a Francoforte, con le copie di sicurezza in Irlanda e i modelli di intelligenza artificiale su Amazon Bedrock nelle regioni dell'Unione. Pochi componenti, infrastruttura descritta come codice, secondo fattore obbligatorio per tutti, ogni rilascio dopo una verifica automatica che comprende la scansione dei segreti e una prova di ripristino.

UE
Dati, copie, modelli ed embeddings nelle regioni AWS dell'Unione

TOTP
Secondo fattore obbligatorio per ogni utente e su ogni console amministrativa

24 h · 8 h
RPO e RTO nella stessa regione, con prova di ripristino trimestrale

2 ore
Prima notifica di un incidente TIC al Cliente

72 ore
Correzione delle vulnerabilità critiche

90 gg · 12 m
Log di accesso e applicativi; log di sicurezza e amministrazione

Infrastruttura e accessi

- **Cifratura a riposo** dei dischi e delle copie (AWS KMS, AES-256); HTTPS con TLS 1.2-1.3, HSTS di un anno e intestazioni di sicurezza.
- **Login su invito** con Amazon Cognito, TOTP obbligatorio, token verificato a ogni richiesta; ruoli imposti dal server.
- **Isolamento tra studi** con un unico predicato di visibilità, coperto da test automatici; cache OCR per studio.
- **Nessuna porta SSH**; amministrazione con AWS Systems Manager, sessioni registrate, credenziali solo temporanee.
- **CloudTrail** su tutte le regioni con convalida dell'integrità, **GuardDuty**, sonda esterna ogni minuto e allarmi 24/7.

Dati, modelli e resilienza

- **Modelli Claude su Amazon Bedrock UE**: il produttore del modello non riceve i dati, nessun addestramento sui dati dei clienti.
- **Embeddings nell'UE** (Amazon Titan); nessun embedding sui fascicoli penali.
- **Rilasci** solo con verifica superata: tipi, test, scansione dei segreti, prova di ripristino; branch di ambiente protetti.
- **Copie giornaliere** cifrate, 14 a Francoforte e 14 in Irlanda; prova di ripristino trimestrale con verbale.
- **Cancellazione completa** a fine contratto, cache e conversazioni comprese, con conferma scritta.

Con questo documento

VALUTAZIONE DEL FORNITORE

13 Questionario precompilato · 14 Dichiarazione di applicabilità ISO/IEC 27001 · 15 Registro dei subfornitori · 17 Mappa DORA.

CONTRATTO

07 Accordo sul trattamento dei dati · 18 Allegato DORA · 55 SLA · 56 Piano di uscita · 51 Modelli di notifica.

AUDIT

Politiche P01-P17 · procedure 20-31 · registri 40-45 · verbali delle prove di ripristino, mostrati in sede.

CERTIFICAZIONI

L'infrastruttura è certificata da AWS (ISO/IEC 27001, 27017, 27018, SOC 2, C5), con i rapporti da AWS Artifact su richiesta. Il percorso di Trailgun verso la certificazione ISO/IEC 27001:2022, il primo penetration test indipendente e la nuova piattaforma su più zone sono descritti, con le date, nel documento 12.

ENGLISH SUMMARY

Information security at a glance

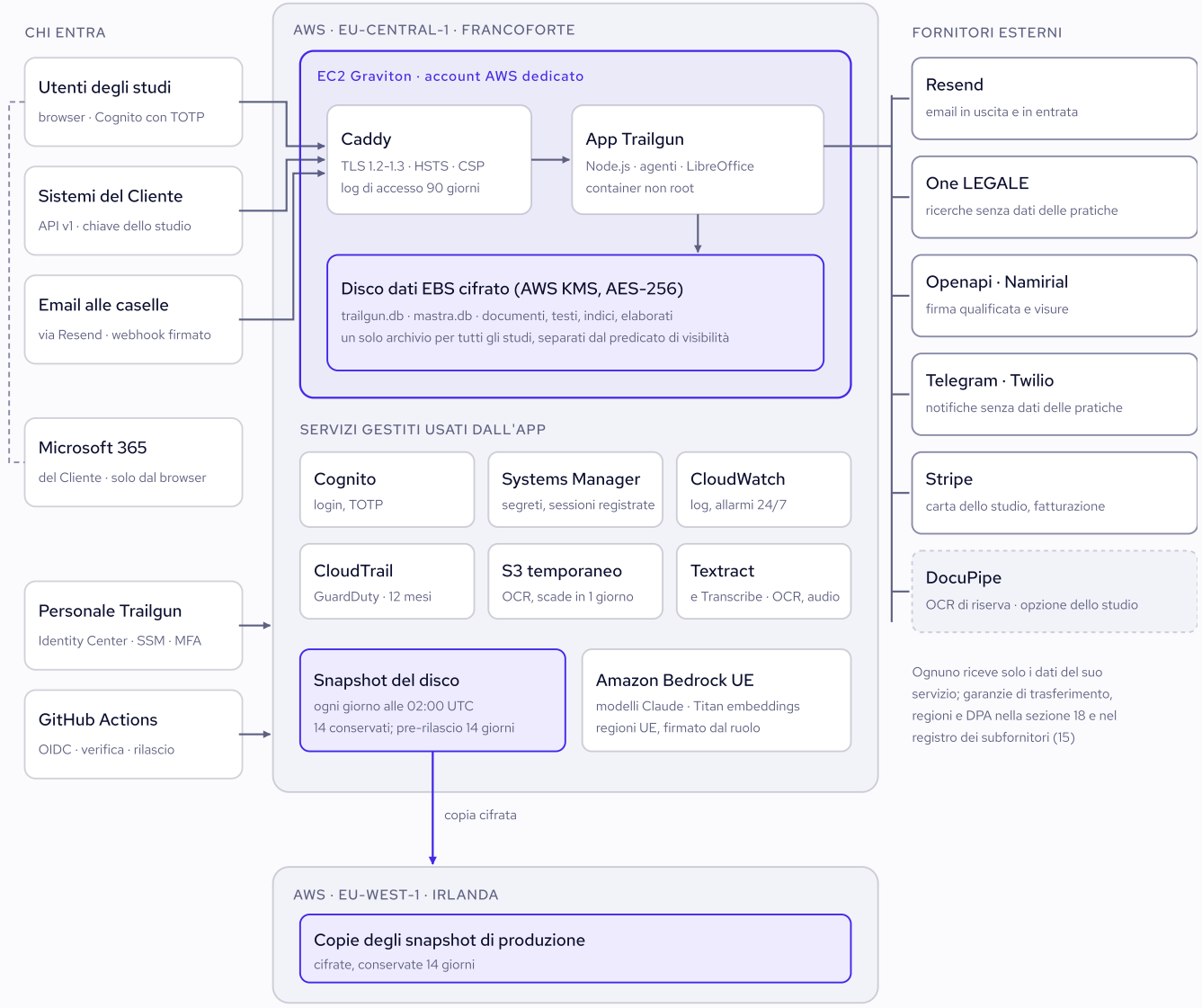
This page summarises the Italian document for international reviewers. It reflects the production code and AWS configuration as of 1 December 2026. Every control listed is in place, with evidence available for audit. Future milestones carry a code (R01–R17) and are dated in document 12, «Certification and platform roadmap».

AREA	POSITION	STATUS
Hosting	AWS eu-central-1 (Frankfurt), dedicated AWS account in AWS Organizations; one EC2 instance per environment; two SQLite databases and files on an encrypted EBS volume; infrastructure as code (AWS CDK)	IN PLACE
Identity	Amazon Cognito, invitation only, mandatory TOTP MFA for every user, token verified on every API request; roles admin, member, operator and viewer enforced server-side; MFA on every administrative console; temporary admin credentials (IAM Identity Center)	IN PLACE
Tenant isolation	Logical: one visibility predicate for every query on client data, automated multi-tenant tests before each release; OCR cache scoped per firm and deleted with the case	IN PLACE
Encryption	AES-256 at rest (EBS, snapshots, S3) with AWS KMS; TLS 1.2-1.3 in transit, HSTS for one year, CSP and security headers	IN PLACE
AI models	All agents on Anthropic Claude through Amazon Bedrock in EU regions, signed by the instance role; non-EU regions refused by code; embeddings with Amazon Titan in the EU; no training on client data; AWS AI services opt-out policy	IN PLACE
Logging	HTTP access and application logs 90 days, no request bodies or tokens; CloudTrail in all regions with integrity validation and SSM session logs, 12 months; GuardDuty; external probe every minute with 24/7 alerts	IN PLACE
Backup	Daily snapshot at 02:00 UTC, 14 retained, encrypted copy in eu-west-1 (Ireland) kept 14 days; pre-release snapshots expire after 14 days	IN PLACE
Recovery	RPO 24 h, RTO 8 h in region; restore drill in CI on every check and quarterly on the real snapshot with a record and measured RTO. Shorter RPO and regional RTO: roadmap R01, R03, R14	IN PLACE
Availability	99.5% monthly 24/7 and 99.8% in business hours, measured every minute by the external probe; higher levels with the new platform (R12, R14)	contractual
Incidents	First notice within 2 hours, updates every 24 hours, intermediate report within 48 hours, final report within 20 days of closure; personal data breaches notified to the controller within 24 hours	contractual
Secure development	Protected environment branches; release only after typecheck, unit and end-to-end tests, secret scanning (gitleaks, full history) and restore drill, also for manual releases; Dependabot, ECR scanning; fixes critical 72 h, high 7 d, medium 30 d, low 90 d	IN PLACE
Criminal files	No embeddings; every consultation, question, analysis, timeline, graph and defendant sheet logged; text processed only on Bedrock EU	IN PLACE
Certification	AWS certifications for the infrastructure. Trailgun: independent penetration test (R06), ISO/IEC 27001 gap assessment, ISMS, stage 1 and certificate (R07, R08, R15, R16), source-code escrow (R09)	roadmap
Audit	One audit a year with 30 days' notice; unlimited access, inspection and audit for DORA critical or important functions and for authorities (Art. 30(3)(e) DORA)	contractual

Contacts: security@trailgun.ai (24/7 for priority 1) and privacy@trailgun.ai. Responsible disclosure: https://trailgun.ai/security and https://trailgun.ai/.well-known/security.txt. Sub-processors: https://trailgun.ai/subprocessors.

FIGURA 1 · ARCHITETTURA DI PRODUZIONE AL 01/12/2026

Un host, un disco cifrato, i modelli nell'Unione



Il tratteggio a sinistra fra gli utenti e Microsoft 365 indica che il file della revisione in Word va dal browser dell'avvocato al suo tenant: il server Trailgun non vede le credenziali Microsoft. Le email in arrivo raggiungono l'app attraverso Resend con un webhook firmato. Le chiamate ai modelli partono dal server firmate dal ruolo dell'istanza e il codice rifiuta ogni regione fuori dall'Unione.

DOVE STANNO I DATI

Sul disco cifrato a Francoforte; copie cifrate anche in Irlanda. File per OCR e audio su S3 per al massimo un giorno.

CHI PUÒ ENTRARE

Dalla rete solo HTTPS. Gli utenti con secondo fattore; i sistemi con la chiave API; il personale solo attraverso AWS, con credenziali temporanee.

CHE COSA ESCE

Email approvate, notifiche senza dati delle pratiche, ricerche giuridiche filtrate, documenti da firmare: sezioni 5 e 18.

SEZIONE 1

Scopo, ambito e destinatari

Che cosa descrive il documento, per chi, e come si legge.

1.1 Scopo

Il documento descrive le misure di sicurezza delle informazioni della piattaforma Trailgun, dei processi che la gestiscono e dei fornitori su cui poggia. Serve agli uffici di sicurezza, IT, rischio dei fornitori, protezione dei dati e conformità di banche, intermediari finanziari iscritti all'albo dell'art. 106 TUB, servicer e studi legali, per la valutazione del fornitore prima del contratto (art. 28, par. 4, Reg. (UE) 2022/2554, «DORA») e per la verifica delle garanzie sufficienti del responsabile del trattamento (art. 28, par. 1, e art. 32 Reg. (UE) 2016/679, «GDPR»).

1.2 Ambito

a) Dentro l'ambito: l'applicazione app.trailgun.ai, il pannello della piattaforma backoffice.trailgun.ai, l'interfaccia di programmazione pubblica (`/api/v1`), il sito trailgun.ai servito dallo stesso server; l'ambiente di produzione e, per quanto incide sulla produzione, gli ambienti di staging e development, la catena di sviluppo e rilascio, i fornitori che trattano dati o sostengono il servizio.

b) Fuori dall'ambito: i dispositivi, le reti, le caselle di posta e le credenziali del Cliente; il tenant Microsoft 365 del Cliente usato per la revisione in Word, che il browser dell'avvocato raggiunge direttamente; i sistemi dei fornitori oltre a quanto dichiarato nei loro attestati.

1.3 Fonte dei fatti e degli impegni

I fatti sulla piattaforma corrispondono al codice in produzione e alla configurazione dell'account AWS al 01/12/2026, riletti prima della pubblicazione di questa versione. Gli impegni (livelli di servizio, RPO, RTO, tempi di notifica, conservazione) provengono da un'unica tabella, la stessa usata dal Contratto di servizio, dall'Accordo sul trattamento dei dati (documento 07), dal documento 08 sulla DORA, dall'Accordo sul livello di servizio (documento 55) e dalle politiche P01–P17: un numero di questo documento è identico in tutti gli altri.

1.4 Stato dei controlli

Ogni controllo descritto è IN ESSERE alla data del documento, con un'evidenza che si mostra in sede di audit: configurazione, codice e test, verbali delle prove, registri 40–45. Le poche tappe successive, cioè la certificazione ISO/IEC 27001, i test di terze parti, il deposito del codice e la nuova piattaforma su più zone, sono richiamate con il loro codice PERCORSO R01–R17 e hanno data ed evidenza attesa nel documento 12, Percorso di certificazione e piattaforma. L'Allegato A elenca tutti i controlli; l'Allegato B rinvia alle politiche, alle procedure e ai registri che li governano.

1.5 Riservatezza e aggiornamento

Il documento contiene informazioni sulla sicurezza della piattaforma e va condiviso solo con le persone coinvolte nella valutazione. Identificativi di risorse, indirizzi e nomi di account non sono riportati: si mostrano in sede di audit. Il documento si aggiorna dopo ogni incidente grave o cambiamento rilevante dell'architettura, a ogni tappa del Percorso raggiunta e almeno una volta l'anno; la versione in vigore è sempre quella indicata nel Trust Center (documento 00).

SEZIONE 2

Governance, ruoli e responsabilità

Chi risponde della sicurezza, come si raggiunge, chi fa che cosa tra Trailgun, il Cliente e AWS.

2.1 La società

[Trailgun S.r.l.], sede legale [indirizzo], P.IVA e C.F. [...], Registro delle imprese e REA [...], PEC [...], capitale sociale [...]. Codice LEI per il registro delle informazioni DORA (Reg. di esecuzione (UE) 2024/2956, modello B_05.01): [LEI]; i dati per il registro sono raccolti nella Scheda per il Registro delle informazioni (documento 16). Legale rappresentante: Franco Puppo, CEO. Il cofondatore Alessandro Musella, avvocato, cura il metodo e il legal design del prodotto e non ha ruoli esecutivi.

2.2 Responsabilità della direzione

L'organo amministrativo ha la responsabilità ultima della sicurezza delle informazioni: approva questo documento, le politiche P01-P17 e la politica di governance dell'IA, assegna le risorse, riceve la relazione su ogni incidente grave e decide il trattamento dei rischi registrati nel Registro dei rischi ICT (documento 41). Franco Puppo, CEO, è il responsabile della sicurezza; la nomina di un responsabile dedicato è la tappa R13 del Percorso.

2.3 Ruoli e contatti

RUOLO	CHI	NOTE
Legale rappresentante e referente contrattuale	Franco Puppo, CEO · [email]	IN ESSERE
Responsabile della sicurezza	Franco Puppo, CEO	responsabile dedicato: PERCORSO R13
Responsabile della protezione dei dati (DPO)	[DPO esterno: nome o società], dpo@[...]	nominato e comunicato al Garante (art. 37, par. 7, GDPR)
Responsabile della conformità IA	[nome]	politica P15, documento 09
Sicurezza e incidenti	security@trailgun.ai	presidiata 24/7 per la priorità 1, risposta automatica con il numero di reperibilità
Privacy	privacy@trailgun.ai	richieste del Titolare, degli interessati, del DPO
Reperibilità priorità 1	[+39 ...]	24/7, solo priorità 1
Assistenza	in app (cuffie nella barra in alto: agente e ticket) e info@trailgun.ai	giorni lavorativi 09:00-18:00

2.4 Separazione dei compiti e persona chiave

Trailgun è una società giovane e l'accesso tecnico alla produzione è concentrato nel CEO. Il rischio è registrato nel Registro dei rischi ICT (documento 41) ed è trattato con controlli che non dipendono dalla buona fede di chi ha l'accesso:

- branch di ambiente protetti e rilascio solo con verifica automatica superata, anche quando il rilascio di produzione è lanciato a mano (sezione 10) IN ESSERE;
- registro delle attività amministrative su AWS (CloudTrail su tutte le regioni con convalida dell'integrità, sessioni Systems Manager) conservato 12 mesi, fuori dalla portata dell'applicazione IN ESSERE;
- credenziali amministrative solo temporanee con IAM Identity Center e secondo fattore, nessuna chiave statica IN ESSERE;
- revisione trimestrale degli accessi privilegiati verbalizzata (procedura 22, modello 44) IN ESSERE;
- infrastruttura descritta come codice, runbook di ripristino scritto e provato, accesso di emergenza con un depositario (documento 11) IN ESSERE;
- deposito del codice sorgente presso un agente terzo PERCORSO R09 e responsabile della sicurezza dedicato PERCORSO R13.

2.5 Modello di responsabilità condivisa

La sicurezza del servizio si divide fra tre soggetti. Il Cliente resta pienamente responsabile dei propri obblighi DORA anche quando usa servizi TIC di terzi (art. 28, par. 1, lett. a, DORA).

SOGGETTO	RESPONSABILITÀ
AWS	Sicurezza fisica dei data center, hardware, rete di base, virtualizzazione, servizi gestiti (Cognito, KMS, S3, Bedrock, Textract, Transcribe, CloudWatch, CloudTrail, GuardDuty, Systems Manager), secondo il modello di responsabilità condivisa di AWS e le sue certificazioni.
Trailgun	Applicazione e suo codice, configurazione dell'infrastruttura, sistema operativo e container, gestione delle identità della piattaforma, cifratura, segreti, log, backup e ripristino, monitoraggio, gestione delle vulnerabilità e degli incidenti, scelta e controllo dei subfornitori, formazione del proprio personale.

SOGGETTO	RESPONSABILITÀ
Cliente	Abilitazione e disattivazione dei propri utenti, ruoli e visibilità dei clienti dello studio, custodia delle credenziali, dell'app di autenticazione e delle chiavi API, sicurezza dei propri dispositivi e caselle, liceità dei documenti caricati, revisione degli elaborati prima dell'uso; per i clienti DORA, la qualificazione della funzione supportata (art. 3, punto 22), il registro delle informazioni e le segnalazioni all'autorità.

2.6 Politiche e procedure

Il quadro è adottato dall'organo amministrativo il [data] e si rivede ogni anno. Le politiche sono raccolte nel documento 10; ognuna è anche un documento a sé.

CODICE	POLITICA	PROCEDURE E REGISTRI COLLEGATI
P01	Sicurezza delle informazioni	questo documento; dichiarazione di applicabilità 14
P02	Gestione del rischio ICT	Registro dei rischi ICT 41
P03	Controllo degli accessi	procedure 21, 22; modello 44
P04	Crittografia e gestione delle chiavi	procedura 23
P05	Sicurezza delle operazioni e gestione dei cambiamenti	procedura 20; registro 45
P06	Sviluppo sicuro	procedura 20
P07	Gestione delle vulnerabilità	procedura 24
P08	Logging e monitoraggio	procedura 25
P09	Backup e ripristino	procedure 30, 31
P10	Gestione dei fornitori ICT	procedura 29; registro 15
P11	Classificazione e trattamento delle informazioni	inventario degli asset 42
P12	Conservazione e cancellazione	procedura 28; certificati 53, 54
P13	Sicurezza del personale e formazione	procedura 21; registro 43
P14	Uso accettabile	dispositivi e strumenti del personale
P15	Governance dell'intelligenza artificiale	documento 09; mappa 47
P16	Fascicoli penali: regime rafforzato	sezione 19
P17	Gestione delle segnalazioni (whistleblowing)	canale interno

2.7 Gestione del rischio

I rischi ICT si valutano con il metodo della politica P02 (impatto per probabilità, rischio inerente e residuo, titolare, trattamento) e stanno nel Registro dei rischi ICT (documento 41), rivisto ogni anno e a ogni cambiamento rilevante. Ogni nuovo verticale o funzione nasce come opzione spenta: spenta, il flusso resta identico a prima, e la scelta si congela sull'atto alla creazione. Il rischio di un cambiamento resta così confinato a chi lo attiva.

SEZIONE 3

SGSI e percorso ISO/IEC 27001

Il sistema di gestione in essere, le certificazioni dell'infrastruttura e le garanzie che il Cliente può usare nella valutazione.

3.1 Il sistema di gestione

La sicurezza si governa con le diciassette politiche P01-P17, le dodici procedure 20-31, i registri 40-45 e la dichiarazione di applicabilità rispetto all'Allegato A di ISO/IEC 27001:2022 (documento 14), che riporta per ogni controllo lo stato e l'evidenza. L'infrastruttura è certificata da AWS (ISO/IEC 27001, 27017, 27018, SOC 2, C5). Il percorso verso la certificazione di Trailgun, con l'ambito «piattaforma Trailgun e processi di supporto», è nel documento 12: gap assessment (R07), sistema di gestione definitivo (R08), audit di stage 1 (R15), certificato (R16) e valutazione di ISO/IEC 42001 (R17).

3.2 Le garanzie per la valutazione del Cliente

Il Cliente fonda la propria valutazione sugli elementi che il Reg. delegato (UE) 2024/1773, art. 6, par. 3, ammette come prova: audit del Cliente, rapporti indipendenti, audit interni del fornitore, informazioni fornite dal fornitore. Trailgun offre:

- questo documento e l'intero pacchetto di conformità, con le evidenze mostrabili in audit;
- un audit ordinario all'anno e, per i clienti DORA con funzioni essenziali o importanti, diritti di accesso, ispezione e audit illimitati (sezione 21; modulo di richiesta 52);
- il verbale delle prove di ripristino, con l'RTO misurato, al Cliente che lo chiede e sempre ai clienti DORA;
- il questionario fornitore precompilato (documento 13) e la risposta ai questionari del Cliente entro 15 giorni lavorativi, una volta l'anno senza costi;
- i rapporti di AWS (ISO/IEC 27001, 27017, 27018, SOC 2, C5), da AWS Artifact su richiesta: coprono l'infrastruttura AWS, non i controlli di Trailgun;
- la sintesi del penetration test indipendente e del piano di rimedio, dal primo test (Percorso R06).

3.3 Altri standard

SOC 2, ISO 22301 e ISO/IEC 27701 non sono nel Percorso. Se un cliente li chiede, li valutiamo insieme a lui, partendo dai controlli già mappati nell'Allegato A e nella dichiarazione di applicabilità.

SEZIONE 4

Architettura

Componenti, ambienti, archivi dei dati, regioni ed evoluzione. La figura 1, prima della sezione 1, ne dà la vista d'insieme.

4.1 Vista d'insieme

Trailgun è un'unica applicazione Node.js (Hono per il server, Mastra per gli agenti, React per l'interfaccia servita dallo stesso server) in un container Docker, su una sola istanza EC2 Graviton per ambiente (in produzione `t4g.large`), in una zona di disponibilità della regione AWS eu-central-1, Francoforte. Nello stesso container girano LibreOffice, per convertire gli atti in PDF/A, e Chromium, per il PDF del faldone e la sessione sulla banca dati One LEGALE. Davanti all'app, sulla stessa macchina, Caddy termina HTTPS. Lo stato del servizio sono due database SQLite e dei file su un disco EBS cifrato dedicato (50 GiB in produzione): i documenti non stanno su S3, che si usa solo come appoggio temporaneo per OCR e trascrizione. I modelli di intelligenza artificiale girano su Amazon Bedrock nelle regioni dell'Unione. Un solo host serve il sito, l'app e il backoffice e sceglie in base al nome a dominio richiesto.

4.2 Componenti

COMPONENTE	CHE COSA È	NOTE DI SICUREZZA
App	Node.js 24 su immagine base fissata (`node:24.22.1-bookworm-slim`), Hono, Mastra, React; LibreOffice e Chromium nello stesso container	container eseguito con un utente non privilegiato
Reverse proxy	Caddy 2 su immagine fissata a una versione: HTTPS con certificati Let's Encrypt, HTTP/3, redirect da HTTP a HTTPS, intestazioni di sicurezza	log di accesso su CloudWatch, 90 giorni
Host	EC2 `t4g.large` in produzione, `t4g.medium` in staging e development; Amazon Linux 2023 con AMI fissata e aggiornata ogni mese; disco di sistema 30 GiB gp3 cifrato	IMDSv2 obbligatorio; nessuna porta SSH
Disco dati	EBS gp3 cifrato con AWS KMS, 50 GiB in produzione, protetto dalla cancellazione accidentale con lo stack	snapshot giornalieri e copia in Irlanda
Modelli	Amazon Bedrock nelle regioni UE: modelli Claude di Anthropic per gli agenti, Amazon Titan Text Embeddings V2 per la ricerca	richieste firmate dal ruolo dell'istanza; regioni fuori dall'UE rifiutate dal codice
Rete	Security group: in ingresso solo TCP 80, TCP 443, UDP 443; indirizzo IP elastico; DNS su Route 53	sezione 9
Immagini	Amazon ECR per ambiente, ultime 15 immagini	scansione delle vulnerabilità a ogni caricamento

COMPONENTE	CHE COSA È	NOTE DI SICUREZZA
Segreti	AWS Systems Manager Parameter Store, parametri SecureString per ambiente	sul server in un file leggibile solo dal proprietario; rotazione annuale
Login	Amazon Cognito, un pool per ambiente	sezione 7
Archivio temporaneo	Bucket S3 per Textract e Transcribe: cifratura lato server, accesso pubblico bloccato, solo TLS, scadenza a 1 giorno; l'app cancella il file a fine analisi	IN ESSERE
Log e rilevazione	CloudWatch Logs (accessi e applicazione 90 giorni); CloudTrail su tutte le regioni con convalida dell'integrità, 12 mesi; GuardDuty; allarmi CloudWatch	sezione 12
Copie	Amazon Data Lifecycle Manager: snapshot giornaliero, copia cifrata in eu-west-1; snapshot prima di ogni rilascio con scadenza a 14 giorni	sezione 13
Posta	Amazon SES come mittente delle email di Cognito; Resend per le email dell'app; Google Workspace per le caselle delle persone	SPF, DKIM e DMARC pubblicati (sezione 9.3)
CI	Stack dedicato con provider OIDC di GitHub e un ruolo per ambiente	sezione 10

4.3 Ambienti

Ogni ambiente ha macchina, disco, indirizzo IP, archivio delle immagini, parametri, log, bucket e pool di utenti propri. Condividono l'account AWS, la regione, la VPC predefinita e la zona DNS. Lo script di rilascio impone in staging e development il pool del proprio stack: un file di configurazione copiato dalla produzione non fa entrare gli utenti veri.

AMBIENTE	INDIRIZZO	BRANCH	SERVIZI ESTERNI	SNAPSHOT
production	app.trailgun.ai	`production`	reali	14 + copia in Irlanda
staging	app.staging.trailgun.ai	`staging`	simulati di default (One LEGALE, email, Telegram, SMS); Openapi in prova	7
development	app.dev.trailgun.ai	`development`	simulati di default	3

4.4 Account AWS

Tutti gli ambienti stanno in un account AWS dedicato e intestato a Trailgun, nella regione eu-central-1, all'interno di AWS Organizations. Una policy dell'organizzazione esclude i contenuti di Textract, Transcribe e Bedrock dal miglioramento dei servizi di IA di AWS (sezione 20.3) IN ESSERE.

4.5 Archivi dei dati

Tutto sta sul disco dati, cifrato a livello di volume. Non c'è una cifratura applicativa aggiuntiva dei database o dei file (sezione 8.1). Alla cessazione del contratto ogni archivio dello studio si cancella (sezione 14.4).

ARCHIVIO	CONTENUTO	CANCELLAZIONE
Database principale (`trailgun.db`)	Utenti, studi, clienti, pratiche, metadati e sintesi dei documenti, dati estratti, versioni degli atti, comunicazioni, attività, notifiche, costi, fatture, impronte delle chiavi API, ticket, memorie, trattative	con la pratica o il cliente; eventi di costo scollegati dai contenuti
Conversazioni con gli agenti (`mastra.db`)	Thread e messaggi degli agenti	con la pratica
Cartella della pratica	Originali dei documenti, testi estratti, indice di ricerca (embeddings Titan, mai sui fascicoli penali), elaborati, faldone	con la pratica
Cache OCR e del layout	Testo e layout riconosciuti da Textract, con chiave che lega studio e contenuto: mai riusati fra studi	con la pratica
Archivio One LEGALE	Fonti giuridiche scaricate dalla banca dati, deduplicate per indirizzo, senza dati delle pratiche	a fine contratto, con lo studio

ARCHIVIO	CONTENUTO	CANCELLAZIONE
Materiali, lotti, arrivi, fatture	Materiali di studio, cliente, avvocato; archivi dei lotti; arrivi da caselle e API; PDF e XML delle fatture	funzioni dedicate; fatture 10 anni
Copie di migrazione	Copia del database principale prima di ogni migrazione, ultime 5, sullo stesso disco	a rotazione e a fine contratto
Certificati	Certificati TLS di Caddy	rinnovo automatico

4.6 Regioni

a) Dati a riposo: Germania (eu-central-1). Copie di sicurezza della produzione: anche Irlanda (eu-west-1).

b) File temporanei per OCR e trascrizione: S3 eu-central-1, al massimo 1 giorno; Textract e Transcribe in eu-central-1.

c) Elaborazione con i modelli ed embeddings: Amazon Bedrock nella regione di Francoforte (eu-central-1). Il codice rifiuta una regione fuori dall'Unione prima che un byte lasci il server IN ESSERE.

d) Fornitori accessori e garanzie di trasferimento: sezione 18 e Registro dei subfornitori (documento 15); localizzazione dei dati: Dichiarazione del documento 61.

4.7 Resilienza dell'architettura ed evoluzione

L'architettura è volutamente semplice: un host per ambiente, un disco, lo stato in SQLite, l'infrastruttura ricostruibile dal codice. La resilienza oggi viene dalle copie (giornaliere, in Irlanda, prima di ogni rilascio), dal runbook di ripristino provato ogni trimestre, dalla sonda esterna con gli allarmi 24/7 e dalla regola per cui il rilascio non parte mentre ci sono lavorazioni del modulo in corso (quelle in coda ripartono da sole). Su questa base valgono i livelli di servizio della sezione 14.2. La nuova piattaforma su più zone di disponibilità, con container senza stato dietro un bilanciatore con AWS WAF, database gestito con ripristino a un istante, file su S3 con versioning e chiavi KMS gestite da Trailgun, è la tappa R12 del Percorso; i nuovi livelli di servizio che ne derivano sono la tappa R14.

SEZIONE 5

Flussi dei dati per canale

Come i documenti entrano, che cosa succede durante la lavorazione, dove escono. Tutte le pratiche nascono da un'unica funzione di creazione, con le regole del loro tipo.

5.1 I quattro canali d'ingresso

CANALE	COME ENTRA	AUTENTICAZIONE	CONTROLLI
Modulo dell'app	Caricamento dal browser su HTTPS, archivio zip o file; la lavorazione parte subito	Token Cognito verificato a ogni richiesta	Fino a 5.000 file per archivio e limite di dimensione (500 MB predefiniti) contro gli archivi malevoli
Lotti	Zip di zip, una pratica per sotto-archivio, in coda	Token Cognito	Limiti propri dei lotti; numero di lavorazioni parallele fissato dalla piattaforma
Caselle email	Indirizzo dello studio con token (`nuova-<token>@` o `<tipo>-<token>@mail.trailgun.ai`); Resend riceve e passa la mail all'app con un webhook firmato; in coda	Token della casella e mittente: mail da mittenti non riconosciuti trattenute finché un utente non le approva	Operatori e viewer non aprono pratiche; lo smistatore è un agente che legge la mail, con il costo intestato all'atto quando nasce
API pubblica	REST su HTTPS, `/api/v1`, descritta in OpenAPI; in coda	Chiave API dello studio (si conserva solo l'impronta SHA-256), che agisce per conto di un utente	120 richieste al minuto per chiave; webhook in uscita firmati HMAC-SHA256

5.2 La lavorazione

1. **Estrazione del testo.** Word ed Excel in locale; PDF e immagini con Amazon Textract, tramite il bucket temporaneo. Il testo riconosciuto si conserva nella cache OCR dello studio. La riserva DocuPipe, negli Stati Uniti, è un'opzione dello studio spenta di default: solo lo studio che la accende manda a DocuPipe i singoli file che Textract non legge.
2. **Audio** dell'analisi del faldone: Amazon Transcribe in eu-central-1, con parlanti distinti.

3. **Agenti.** Ogni chiamata ai modelli va ad Amazon Bedrock nella regione UE, firmata con le credenziali temporanee del ruolo dell'istanza: nessuna chiave di un fornitore di modelli sul server. Un'unica funzione del codice registra modello, agente, token e costo, mai il testo.
4. **Embeddings** per la ricerca «veloce» dell'analisi del faldone: Amazon Titan Text Embeddings V2 su Bedrock nella regione UE, salvati nella cartella dell'atto; senza embeddings la ricerca resta lessicale (BM25). Mai sui fascicoli penali o misti.
5. **Ricerca fonti e verifica giurisprudenziale**: un browser automatizzato interroga One LEGALE con l'account di Trailgun. Una regola in codice, coperta da test, toglie dalle stringhe di ricerca nomi, codici fiscali, importi e altri dati delle pratiche prima che partano.
6. **Comunicazioni con i clienti dello studio** e trattative: email con Resend; le risposte tornano con un webhook firmato (allegati fino a 25 MB, 20 per messaggio). Di default ciò che va all'esterno lo prepara un agente e lo approva l'avvocato; nella modalità automatica, che sceglie lo studio, la mail dice al destinatario che l'ha preparata e inviata un agente di IA per conto dello studio.
7. **Firma qualificata e visure** con Openapi (firma con Namirial), nell'ambiente di produzione del fornitore, con callback firmata.
8. **Revisione in Word**: il file va dal browser dell'avvocato a OneDrive o SharePoint del suo tenant Microsoft; il server di Trailgun non vede le credenziali Microsoft.
9. **Notifiche esterne**: email, Telegram, SMS e WhatsApp portano solo l'avviso e il link all'app, senza dati delle pratiche; il contenuto si legge in app, dopo il login.
10. **Fatturazione**: per gli studi con fatturazione a consumo, la carta si tokenizza su Stripe da chi la inserisce; Trailgun conserva solo il riferimento e le ultime quattro cifre.

5.3 Le uscite

Gli elaborati escono solo per azione di un utente: download dal browser (DOCX, PDF/A, zip del faldone o del pacchetto di deposito con le impronte SHA-256 dei file), webhook dell'API verso i sistemi del Cliente, email di comunicazione approvate. I DOCX e i PDF prodotti dagli agenti portano la marcatura leggibile da macchina dell'art. 50 AI Act (sezione 20.5). Il deposito telematico resta all'avvocato. Il sito e l'app non caricano risorse esterne (font, CDN) e non usano strumenti di analisi o profilazione; il sito non usa cookie.

5.4 Chi in Trailgun vede che cosa

a) **Amministratori della piattaforma** (gruppo Cognito dedicato, sul backoffice): studi, utenti, impostazioni, costi, elenco delle pratiche e ricerche recenti di tutti gli studi, cioè metadati come titoli, stati e costi. Non aprono il contenuto delle pratiche di uno studio: il predicato di visibilità vale anche per loro.

b) **Operatori dell'assistenza** (gruppo dedicato): solo i ticket e la knowledge base.

c) **Accesso al server**: chi ha credenziali amministrative AWS legge database e file, perché la cifratura è a livello di volume. L'accesso è di una persona, con credenziali temporanee e secondo fattore; ogni sessione Systems Manager è registrata e ogni azione su AWS è in CloudTrail. L'accesso ai contenuti delle pratiche è ammesso solo su richiesta del Cliente o per un incidente, e si annota nel registro degli accessi del personale, che il Cliente può chiedere in estratto.

SEZIONE 6

Isolamento tra studi

Un isolamento logico, con un solo punto di controllo e test che lo verificano prima di ogni rilascio.

6.1 Il modello

Tutti gli studi stanno in un unico database. Ogni utente appartiene a un solo studio; i clienti sono dello studio e non si condividono mai fra studi. Ogni interrogazione su dati di un cliente passa da un unico predicato di visibilità, che il codice non replica a mano altrove: la regola è scritta una volta e si verifica in un punto solo. Una suite di test dedicata all'isolamento fra studi gira a ogni rilascio insieme alle altre verifiche obbligatorie IN ESSERE.

6.2 Dentro lo studio

Ogni cliente dello studio ha una visibilità: tutto lo studio, solo chi l'ha creato, oppure utenti selezionati. Ruoli e permessi (sezione 7.3) limitano ciò che ciascuno può fare. Le regole che lo studio chiede di ricordare (memoria dello studio) restano nello studio: si scrivono nei testi aggiuntivi dello studio, mai nei testi comuni di Trailgun, e quelle proposte da un membro valgono per tutto lo studio solo dopo l'approvazione di un amministratore.

6.3 File, indici e cache

Originali, testi, indici di ricerca ed elaborati stanno nella cartella della pratica, che si cancella con la pratica. La cache OCR, la cache del layout di Textract e la deduplica delle analisi in corso usano una chiave che lega lo studio al contenuto: un testo già estratto si riusa solo dentro lo studio che l'ha prodotto, mai fra studi, e si cancella con la pratica IN ESSERE.

6.4 Che cosa resta comune

a) **Metadati nel backoffice.** Gli amministratori della piattaforma vedono titoli, stati e costi delle pratiche di tutti gli studi (sezione 5.4), non il loro contenuto.

b) **Archivio delle fonti giuridiche.** Le fonti scaricate da One LEGALE sono testi pubblici di giurisprudenza e dottrina, senza dati delle pratiche.

c) **Testi comuni dei prompt.** Sono di Trailgun, uguali per tutti, e non contengono dati di alcuno studio: lo studio aggiunge solo testi propri.

d) **Isolamento logico.** L'isolamento è logico, non fisico: un database o un'istanza per singolo cliente non fanno parte del servizio standard.

SEZIONE 7

Identità e accessi

Gli utenti degli studi, i sistemi che usano l'API, il personale di Trailgun. Autenticazione forte (art. 9, par. 4, lett. d, DORA) e privilegi limitati al necessario (lett. c).

7.1 Utenti degli studi

- Amazon Cognito, un pool per ambiente; account solo su invito, nessuna registrazione libera IN ESSERE.
- Secondo fattore obbligatorio per tutti con app di autenticazione (TOTP) IN ESSERE.
- Protocollo SRP: la password non viaggia e Trailgun non la conserva. Almeno 10 caratteri con maiuscole, minuscole e cifre; password temporanea valida 7 giorni; risposte che non rivelano se un utente esiste; pool protetto dalla cancellazione IN ESSERE.
- Su ogni richiesta all'API dell'app il server verifica il token d'identità (firma sulle chiavi del pool, scadenza, destinatario) e confronta l'utente della richiesta con quello del token; il comportamento è coperto da test IN ESSERE.

7.2 Sessioni e disattivazione

Il token d'identità ha scadenza breve ([1 ora] sul client di produzione). La disattivazione dell'account dal backoffice blocca subito i nuovi accessi; una sessione già aperta dura fino alla scadenza del token. Lo studio disattiva i propri utenti dall'Organizzazione. A fine contratto gli utenti dello studio si cancellano anche in Cognito.

7.3 Ruoli e permessi dello studio

a) **admin** (amministra lo studio), **membro** (lavora le pratiche dei clienti che vede), **operator** (porta avanti le pratiche, non ne crea) e **viewer** (sola lettura: niente scritture, niente assistente, niente esportazione in Word). Le regole dei ruoli sono imposte dal server su ogni richiesta, non solo nascoste nell'interfaccia IN ESSERE.

b) Permessi concessi dall'admin al singolo membro: chiedere l'attenzione dei colleghi, accedere all'Amministrazione (costi e fatture) IN ESSERE.

c) Visibilità per cliente (sezione 6.2) IN ESSERE.

7.4 Accesso tra sistemi

- **Chiavi API dello studio**: prefisso visibile per riconoscerle, si conserva solo l'impronta SHA-256, revoca immediata, ogni chiave agisce per conto di un utente dello studio, 120 richieste al minuto IN ESSERE. La rotazione è dello studio, consigliata ogni 12 mesi.
- **Webhook in entrata** verificati: Svix con tolleranza di 5 minuti per Resend e DocuPipe, segreto condiviso per Openapi e Telegram; senza segreto configurato la rotta risponde con un errore e non accetta nulla IN ESSERE.
- **Webhook in uscita** verso i sistemi del Cliente firmati HMAC-SHA256 con marca temporale, nell'intestazione `Trailgun-Signature` IN ESSERE.
- **Caselle email**: token nell'indirizzo, mittenti non riconosciuti trattenuti fino all'approvazione di un utente IN ESSERE.
- **Modelli**: le chiamate a Bedrock sono firmate con le credenziali temporanee del ruolo dell'istanza; nessuna chiave statica di un fornitore di modelli IN ESSERE.

7.5 Accessi privilegiati di Trailgun

CHI	COME	CHE COSA PUÒ	CONTROLLI
CEO, accesso tecnico alla produzione	IAM Identity Center: credenziali temporanee, secondo fattore	Immagini, parametri, comandi Systems Manager sull'istanza, rilascio dell'infrastruttura, pool Cognito, log, snapshot	CloudTrail, sessioni registrate, revisione trimestrale
GitHub Actions	Ruolo OIDC per ambiente, assumibile solo dal branch omonimo	Caricare l'immagine, aggiornare la versione nei parametri del proprio ambiente, comandi sulla propria istanza, snapshot del proprio volume; non cambia l'infrastruttura	nessuna chiave AWS in GitHub
Amministratori della piattaforma	Gruppo Cognito sul backoffice, con TOTP	Studi, utenti, impostazioni, prompt, metadati di pratiche e costi	revisione trimestrale
Operatori dell'assistenza	Gruppo Cognito, con TOTP	Ticket e knowledge base	revisione trimestrale

7.6 Minimo privilegio

Il ruolo dell'istanza può solo scaricare le immagini, scrivere i log, usare il bucket temporaneo, Textract, Transcribe e i modelli di Bedrock nella regione UE, leggere i parametri del proprio prefisso e gestire gli utenti del proprio pool IN ESSERE. I ruoli della CI sono separati per ambiente e limitati al proprio. Gli accessi amministrativi usano solo credenziali temporanee di IAM Identity Center: non esistono chiavi IAM statiche per il rilascio IN ESSERE.

7.7 Secondo fattore sugli accessi amministrativi

Secondo fattore obbligatorio su AWS (utente root, IAM Identity Center e console), GitHub, con l'obbligo impostato per l'intera organizzazione, Google Workspace, Stripe, Resend e ogni console di fornitore IN ESSERE. La verifica fa parte della revisione trimestrale degli accessi.

7.8 Revisione e revoca

Revisione trimestrale degli accessi privilegiati (AWS, GitHub, backoffice e gruppi Cognito, Google Workspace, console dei fornitori) e degli account di servizio, con l'esito e le correzioni nel modello 44 (procedura 22, Revisione degli accessi) IN ESSERE. Revoca degli accessi del personale entro 24 ore dalla cessazione, con rotazione dei segreti a cui la persona aveva accesso (procedura 21). Lo studio rivede i propri utenti dall'Organizzazione.

7.9 Amministrazione del server

Nessuna porta SSH e nessuna chiave SSH: l'amministrazione passa da AWS Systems Manager (Session Manager e Run Command) con credenziali temporanee. Ogni sessione è registrata e conservata 12 mesi insieme agli eventi di CloudTrail IN ESSERE.

SEZIONE 8

Cifratura e gestione delle chiavi

Dati a riposo, in transito, segreti, integrità. Art. 9, par. 4, lett. d, DORA; art. 6 Reg. delegato (UE) 2024/1774; art. 32, par. 1, lett. a, GDPR. Politica P04 e procedura 23.

8.1 A riposo

Algoritmo AES-256 per tutti i dati a riposo. La cifratura è a livello di volume e di servizio: non c'è una seconda cifratura applicativa dei database o dei file, quindi chi ha accesso amministrativo al server legge i dati in chiaro; per questo quell'accesso è ristretto, temporaneo e registrato (sezione 5.4).

DOVE	COME	STATO
Disco dati e disco di sistema	EBS cifrato con AWS KMS	IN ESSERE
Snapshot in Francoforte e copie in Irlanda	Cifrati; la copia regionale è cifrata nella regione di destinazione	IN ESSERE
Bucket temporaneo	Cifratura lato server S3, accesso pubblico bloccato	IN ESSERE
Segreti	Parameter Store SecureString con la chiave KMS di Systems Manager	IN ESSERE
Chiavi gestite da Trailgun	KMS CMK per database e file, con rotazione annuale attivata, con la nuova piattaforma	PERCORSO R12

8.2 In transito

Solo HTTPS: Caddy ottiene e rinnova da sé i certificati Let's Encrypt (validità 90 giorni), reindirizza HTTP su HTTPS, supporta HTTP/3; i protocolli sono TLS 1.2 e 1.3, con TLS 1.3 preferito. HSTS con durata di un anno IN ESSERE. Verso Bedrock, Textract, Transcribe, il bucket temporaneo (che rifiuta le connessioni senza TLS) e i fornitori esterni sempre HTTPS IN ESSERE.

8.3 Integrità

Il pacchetto di deposito e il faldone portano l'impronta SHA-256 di ogni file. Ogni versione dell'atto conserva autore e motivo, e il testo dell'atto si scrive da un solo punto del codice, così una modifica non passa senza lasciare traccia. I webhook sono firmati in entrambe le direzioni. I log di CloudTrail hanno la convalida dell'integrità IN ESSERE.

8.4 Segreti

I segreti dei fornitori stanno in Parameter Store, mai nel repository, nell'immagine o nel template dell'infrastruttura; lo script di rilascio li scrive e la CI non li cambia; in produzione non arrivano le variabili dei servizi simulati; sul server il file dei segreti è leggibile solo dal proprietario. La scansione dei segreti (gitleaks) controlla l'intera storia del repository a ogni verifica della CI: un segreto trovato blocca il rilascio, si ruota e si toglie dalla storia, mai si mette in eccezione. I segreti dei fornitori ruotano ogni 12 mesi e subito dopo un sospetto di compromissione o l'uscita di una persona con accesso (procedura 23) IN ESSERE.

8.5 Rotazione

ELEMENTO	ROTAZIONE	STATO
Chiavi KMS	Annuale automatica	IN ESSERE
Certificati TLS	Automatica, Let's Encrypt a 90 giorni; allarme sulla scadenza	IN ESSERE
Segreti dei fornitori	Ogni 12 mesi, e subito dopo un sospetto o l'uscita di una persona	IN ESSERE
Credenziali amministrative	Temporanee per costruzione (IAM Identity Center)	IN ESSERE
Chiavi API dello studio	A cura dello studio, consigliata ogni 12 mesi; revoca immediata	IN ESSERE
Password degli utenti	Gestite da Cognito, mai conservate da Trailgun	IN ESSERE

SEZIONE 9

Sicurezza della rete

Una superficie esposta piccola: due porte, nessun accesso amministrativo dalla rete.

9.1 Esposizione

a) In ingresso sono aperte solo TCP 80 (che reindirizza su HTTPS), TCP 443 e UDP 443 (HTTP/3) IN ESSERE. Nessuna porta di amministrazione, database o SSH.

b) Il traffico in uscita non ha un filtro di rete: l'applicazione chiama, solo su HTTPS, i servizi AWS e i fornitori elencati nella sezione 18; GuardDuty segnala le comunicazioni anomale dell'istanza.

c) L'istanza sta in una subnet pubblica della VPC predefinita, con indirizzo IP elastico e solo le porte della lett. a; il bilanciatore con AWS WAF arriva con la nuova piattaforma (Percorso R12).

d) IMDSv2 obbligatorio sull'istanza, contro il furto delle credenziali dal servizio dei metadati IN ESSERE.

9.2 Protezioni applicative

Intestazioni di sicurezza su tutte le risposte: HSTS, Content-Security-Policy, X-Content-Type-Options, Referrer-Policy, frame-ancestors IN ESSERE. Limite di 120 richieste al minuto per chiave sull'API pubblica; il login è delegato a Cognito, con le sue protezioni dai tentativi ripetuti IN ESSERE. Limiti sul numero di voci e sulla dimensione degli archivi caricati IN ESSERE. Un filtro applicativo (AWS WAF) si aggiunge con la nuova piattaforma (Percorso R12).

9.3 Posta e domini

Le email dell'app partono da Resend; quelle di Cognito da Amazon SES. Per i domini di invio sono pubblicati SPF, DKIM e DMARC; la politica DMARC si rende più restrittiva sulla base dei rapporti aggregati.

9.4 Revisione in Word

L'avvocato apre l'atto in Word dal proprio browser, con l'app Microsoft multi-tenant di Trailgun (MSAL con PKCE). Le chiamate a Microsoft Graph partono solo dal browser: il server di Trailgun non vede le credenziali Microsoft e Microsoft non riceve dati da Trailgun IN ESSERE.

SEZIONE 10

Sviluppo sicuro e gestione dei cambiamenti

Dal commit al rilascio: verifiche obbligatorie, branch protetti, nessuna chiave statica, rilasci reversibili. Art. 9, par. 4, lett. e, DORA. Politiche P05 e P06, procedura 20.

10.1 Flusso

Si lavora su un branch, poi richiesta di integrazione verso `development`, quindi `staging` e `production`: ogni branch di ambiente pubblica il proprio ambiente, solo dopo la verifica. I branch di ambiente sono protetti: si aggiornano solo con una richiesta di integrazione e con la verifica superata IN ESSERE. Ogni rilascio di produzione si annota nel Registro dei cambiamenti (documento 45).

10.2 Verifica obbligatoria

Prima di ogni rilascio girano il controllo dei tipi del server, dell'interfaccia e dell'infrastruttura, i test unitari, i test end-to-end nel browser, la scansione dei segreti su tutta la storia del repository e la prova automatica di ripristino delle copie. Fra i test ci sono quelli sull'isolamento fra studi, sulla verifica dei token, sull'API pubblica, sulla fatturazione, sulla regola che toglie i dati delle pratiche dalle ricerche giuridiche e sul rifiuto delle regioni dei modelli fuori dall'Unione. Se una verifica fallisce, il rilascio non parte IN ESSERE. Vale anche per il rilascio di produzione lanciato a mano: lo script rifiuta un commit che non ha la verifica superata.

10.3 Costruzione e rilascio

- Immagine costruita nella CI per arm64, etichettata con il commit, caricata su ECR con scansione delle vulnerabilità IN ESSERE.
- La CI si autentica ad AWS con OIDC: nessuna chiave AWS in GitHub; ogni ruolo vale solo per il proprio branch e il proprio ambiente; l'infrastruttura si cambia solo a mano, nominando lo stack IN ESSERE.
- Il rilascio si rifiuta se ci sono lavorazioni del modulo in corso; la produzione si pubblica solo dal branch `production` pulito; prima di ogni rilascio di produzione si fa uno snapshot del disco dati, conservato 14 giorni; prima di ogni migrazione una copia del database; dopo il riavvio si controlla lo stato di salute IN ESSERE.
- Le migrazioni dello schema sono numerate, solo in avanti, mai modificate dopo la pubblicazione e compatibili con l'immagine precedente IN ESSERE.
- Rilasci ordinari sotto i 2 minuti e solo senza lavorazioni del modulo in corso; una lavorazione interrotta si riavvia senza costi.

10.4 Revisione del codice

Ogni modifica passa da una richiesta di integrazione, con la revisione automatica di agenti di revisione e la verifica obbligatoria della sezione 10.2 come condizione del merge sui branch di ambiente IN ESSERE. Le modifiche che toccano sicurezza, isolamento, costi o dati dei clienti hanno test dedicati, che restano nella suite e girano a ogni rilascio successivo.

10.5 Le novità sono opzioni

Ogni passo nuovo dei flussi si attiva e si disattiva, dalle impostazioni e dal modulo del singolo atto; spento, il flusso resta identico a prima, con lo stesso codice e gli stessi prompt, e la scelta si congela sull'atto alla creazione. Un passo accessorio non fa mai fallire l'atto: a un guasto resta il risultato di prima. È una regola di prodotto applicata a ogni modifica IN ESSERE.

10.6 Dipendenze e ambienti

Dependabot apre ogni settimana le richieste di aggiornamento per i pacchetti npm, le immagini Docker e le GitHub Actions; si integrano dopo la verifica, nei tempi della sezione 11; gli avvisi di sicurezza del repository sono attivi IN ESSERE. Immagini base di Node.js e di Caddy fissate a una versione IN ESSERE. Gli ambienti di staging e development hanno pool, dati e servizi esterni simulati propri IN ESSERE.

10.7 Scansione dei segreti

Il job «secrets» della verifica esegue gitleaks con le regole predefinite su tutta la storia del repository, con i segreti oscurati nel risultato. Le eccezioni sono ammesse solo per falsi positivi dimostrati, ciascuna con la sua motivazione nel file di configurazione; un segreto vero non si mette mai in eccezione: si ruota e si toglie dalla storia (procedura 23) IN ESSERE.

SEZIONE 11

Gestione delle vulnerabilità e patch

Art. 9, par. 4, lett. f, DORA; art. 10 Reg. delegato (UE) 2024/1774. Politica P07, procedura 24.

11.1 Fonti

Le vulnerabilità arrivano da: Dependabot, settimanale; scansione delle immagini su ECR a ogni caricamento; scansione dei segreti a ogni verifica; GuardDuty; bollettini dei fornitori (AWS, Node.js, Caddy, LibreOffice, Chromium); il catalogo CISA delle vulnerabilità sfruttate (KEV); le segnalazioni di terzi a security@trailgun.ai secondo la politica di segnalazione responsabile IN ESSERE. La scansione esterna mensile dell'applicazione e il penetration test indipendente sono le tappe R05 e R06 del Percorso.

11.2 Tempi di correzione

Dalla disponibilità della correzione, per vulnerabilità che toccano componenti in uso; gravità secondo CVSS v3.1 o v4. Vincolanti dalla firma.

GRAVITÀ	CRITERIO	TEMPO	NOTE
Critica	CVSS ≥ 9,0 o sfruttata attivamente (catalogo CISA KEV)	72 ore	mitigazione immediata se la correzione non c'è
Alta	CVSS 7,0-8,9	7 giorni	
Media	CVSS 4,0-6,9	30 giorni	

GRAVITÀ	CRITERIO	TEMPO	NOTE
Bassa	CVSS < 4,0	90 giorni	
Sistema operativo dell'host	Aggiornamenti di sicurezza dell'AMI	mensili	nuova AMI provata in staging, poi in produzione

11.3 File caricati

I file caricati si aprono solo sul server, nel container dell'app eseguito senza privilegi, con pdf.js, LibreOffice e Chromium, e con limiti sul numero di voci e sulla dimensione degli archivi. Non vengono eseguiti, non si servono ad altri studi e non escono se non per azione dell'utente. Una scansione antimalware dedicata non è parte del servizio: il rischio è valutato e accettato nel Registro dei rischi ICT (documento 41), con queste misure.

11.4 Segnalazione responsabile

Chi trova una vulnerabilità la segnala a security@trailgun.ai, secondo la politica pubblicata su https://trailgun.ai/security e nel file https://trailgun.ai/.well-known/security.txt (RFC 9116). La politica tutela il ricercatore in buona fede e fissa i tempi di risposta (procedura 24, Gestione delle vulnerabilità e segnalazione responsabile). La segnalazione si tratta con i tempi della tabella 11.2 e, se ha toccato dati o servizio, come un incidente (sezione 15).

SEZIONE 12

Log e monitoraggio

Che cosa si registra, per quanto, e come ci si accorge di un problema. Art. 10 DORA; art. 12 Reg. delegato (UE) 2024/1774. Politica P08.

12.1 Registri e conservazione

REGISTRO	CONTENUTO	CONSERVAZIONE	NOTE
Accessi HTTP	Registro degli accessi del proxy su CloudWatch	90 giorni	senza corpo delle richieste né token
Log applicativi	Eventi e errori dell'app su CloudWatch	90 giorni	mai testo dei documenti
Log di servizio del proxy	Avvio, certificati, errori	14 giorni	
Sicurezza e amministrazione	CloudTrail su tutte le regioni con convalida dell'integrità, sessioni Systems Manager, accessi al backoffice	12 mesi	fuori dalla portata dell'applicazione
Registro delle attività dello studio	Chi, cosa, quando, su quale cliente o atto	per tutta la durata del contratto	consultabile ed esportabile dall'amministratore dello studio, con la stessa visibilità dei dati
Accessi ai fascicoli penali	Consultazioni (una all'ora per utente), domande, analisi, confronti fra depositi, timeline, grafi, schede degli imputati	per tutta la durata del contratto	sezione 19, esportabile dal Titolare
Accessi del personale ai contenuti	Chi, quando, quale pratica, per quale richiesta o incidente	per tutta la durata del contratto	estratto al Cliente su richiesta
Versioni dell'atto	Autore e motivo di ogni versione	con l'atto	
Eventi di costo	Modello, agente, token, costo; mai il testo	servono alla fatturazione	scollegati dai contenuti alla cancellazione

12.2 Contenuto dei log applicativi

I log applicativi contengono prefissi di modulo, identificativi, nomi di file ed errori, mai il testo dei documenti: i messaggi sono stati rivisti con questa regola e la regola vale per ogni modifica successiva. I nomi dei file possono contenere dati personali e sono trattati come tali. Nessun log contiene password, token o chiavi API.

12.3 Monitoraggio

Una sonda esterna interroga ogni minuto il controllo di salute dell'app e l'avvio di una lavorazione: è anche la misura dei livelli di servizio (sezione 14.2). Gli allarmi, 24/7, coprono salute dell'app, spazio su disco, CPU, memoria, errori 5xx e scadenza dei certificati e raggiungono il reperibile. Amazon GuardDuty analizza CloudTrail, DNS e flussi di rete. La pagina «Sistema» del backoffice mostra versione, dimensione dei database, stato delle migrazioni e spazio su disco IN ESSERE. Il riavvio di produzione fallito il 21/10/2026 per il disco di sistema pieno, un incidente operativo di disponibilità senza perdita né esposizione di dati, è nel registro degli incidenti: l'allarme sullo spazio su disco copre ora quel caso.

12.4 Informazioni al Cliente

- Su richiesta, e sempre per i clienti DORA: esito delle prove di ripristino, estratto del registro degli incidenti che lo riguardano, cambi dei subfornitori, disponibilità del mese misurata dalla sonda IN ESSERE.
- Il rapporto di servizio mensile in app e trimestrale per email (disponibilità, incidenti, ticket e tempi, cambi di subfornitori, prove di ripristino) è la tappa R04 del Percorso.

12.5 Orologi

Sincronizzazione con Amazon Time Sync Service (chrony, predefinito di Amazon Linux 2023), per date e ore coerenti fra i registri IN ESSERE.

SEZIONE 13

Backup e ripristino

Art. 12 DORA; art. 32, par. 1, lett. c, GDPR. Politica P09, procedure 30 e 31.

13.1 Le copie

COPIA	FREQUENZA E CONSERVAZIONE	STATO
Snapshot giornaliero del disco dati	Ogni 24 ore alle 02:00 UTC; 14 conservati in Francoforte (7 in staging, 3 in development)	IN ESSERE
Copia in Irlanda	Ogni snapshot di produzione, cifrato, conservato 14 giorni in eu-west-1	IN ESSERE
Snapshot prima di ogni rilascio di produzione	A ogni rilascio, conservato 14 giorni	IN ESSERE
Copia del database prima di una migrazione	Ultime 5, sullo stesso disco: un aiuto al ritorno indietro, non un backup	IN ESSERE
Snapshot ogni 4 ore	Conservati 7 giorni, in aggiunta al giornaliero	PERCORSO R01
Copie protette dalla cancellazione	EBS Snapshot Lock o AWS Backup Vault Lock per 7 giorni	PERCORSO R11
Nuova piattaforma	Database gestito con ripristino a un istante, file su S3 con versioning, AWS Backup con copie in Irlanda	PERCORSO R12

13.2 Obiettivi di ripristino

RTO in ore di calendario dalla dichiarazione dell'incidente. Sono gli obiettivi che il Cliente confronta con l'RTO e l'RPO della propria funzione (modello B_06.01 del registro delle informazioni). La loro evoluzione è nel documento 12 (tappe R01, R03, R14).

OBIETTIVO	VALORE	COME SI GARANTISCE
RPO	24 ore	Snapshot giornaliero alle 02:00 UTC; nei giorni di rilascio lo snapshot pre-rilascio lo accorcia
RTO nella stessa regione (istanza, disco, zona)	8 ore	Runbook della procedura 30; misurato nella prova trimestrale
Perdita della regione di Francoforte	copie in Irlanda	Procedura regionale e RTO regionale: Percorso R03
Periodo massimo tollerabile di interruzione	5 giorni lavorativi	Assunto nel piano di continuità; il deposito resta possibile all'avvocato con gli elaborati già scaricati

13.3 Il ripristino e la sua prova

Il ripristino segue il runbook della procedura 30: quattro casi (migrazione errata, dati danneggiati con il volume integro, volume perso, regione indisponibile), ciascuno con i suoi passi, la verifica dell'integrità dei database e dei file, la comunicazione agli studi e la misura dei tempi. La prova si fa in due modi IN ESSERE:

- a ogni verifica della CI, una prova automatica ripristina le copie del database e del volume e ne controlla l'integrità;
- ogni trimestre, una prova sullo snapshot reale di produzione, ripristinato in un ambiente isolato, con verbale e RTO misurato (programma 31). La prima prova sullo snapshot reale si è svolta il [data] con un RTO misurato di [hh:mm].

L'esito si comunica al Cliente che lo chiede, sempre ai clienti DORA.

13.4 Il ripristino in Irlanda

Le copie dei dati di produzione sono anche in Irlanda, cifrate, conservate 14 giorni. Lo stack, l'archivio delle immagini, i segreti e il pool degli utenti stanno a Francoforte e si ricreano in Irlanda dall'infrastruttura come codice. La procedura regionale scritta e provata con il suo RTO è la tappa R03 del Percorso; la prova regionale annuale completa è la tappa R10.

13.5 Copie e cancellazione

Tutte le copie hanno una scadenza: i dati cancellati escono dalle copie per rotazione entro 14 giorni dalla cancellazione IN ESSERE.

SEZIONE 14

Continuità operativa

Sintesi del piano di continuità (documento 11). Art. 11 DORA; art. 30, par. 3, lett. c, DORA; artt. 39-40 Reg. delegato (UE) 2024/1774 per il regime semplificato degli intermediari 106.

14.1 Il piano

Il piano di continuità operativa e di ripristino (documento 11, Continuità operativa, ripristino e incidenti) è adottato, con l'analisi d'impatto, gli otto scenari, i ruoli, la reperibilità e la comunicazione di crisi; si rivede e si prova ogni anno. Le prove di ripristino della sezione 13 ne fanno parte IN ESSERE.

14.2 Livelli di servizio

Misurati ogni minuto dalla sonda esterna sul controllo di salute e sull'avvio di una lavorazione. Esclusi la manutenzione programmata, la forza maggiore e i guasti del Cliente o dei servizi esterni che il Cliente sceglie (firma, visure, banche dati). Il testo completo è l'Accordo sul livello di servizio (documento 55); i nuovi livelli della piattaforma su più zone sono la tappa R14.

LIVELLO	IMPEGNO DALLA FIRMA
Disponibilità mensile 24/7	99,5%
Disponibilità mensile nei giorni lavorativi, 08:00-20:00	99,8%
Manutenzione programmata	Preavviso di almeno 48 ore; fra le 20:00 e le 07:00 o nel fine settimana; al massimo 8 ore al mese; interventi urgenti di sicurezza anche senza preavviso, comunicati appena possibile
Crediti di servizio	5% da 99,0% a meno di 99,5%; 10% da 98,0% a meno di 99,0%; 20% da 97,0% a meno di 98,0%; 30% e diritto di recesso sotto il 97,0%. Tetto annuo 30% dei corrispettivi

14.3 Scenari

SCENARIO	RISPOSTA	OBIETTIVO
Guasto dell'istanza, del disco o della zona	Nuova istanza e volume dall'ultimo snapshot, nella stessa regione, dall'infrastruttura come codice (procedura 30)	RTO 8 ore, RPO 24 ore
Perdita della regione di Francoforte	Ripristino in Irlanda dalle copie, ricreando stack, immagini, segreti e pool	Percorso R03
Indisponibilità dei modelli	Gli elaborati già prodotti restano consultabili e scaricabili; le lavorazioni interrotte si riavviano senza costi; i modelli Claude sono disponibili in più regioni UE di Bedrock	–

SCENARIO	RISPOSTA	OBIETTIVO
Indisponibilità di One LEGALE, Openapi o Resend	Il passo accessorio si ferma senza far fallire l'atto; email e caselle in ritardo finché Resend non riprende	escluso dai livelli di servizio se il servizio è scelto dal Cliente
Attacco con cifratura o cancellazione dei dati	Ripristino da snapshot, anche dall'Irlanda; credenziali temporanee e CloudTrail per contenere e ricostruire; copie protette dalla cancellazione: Percorso R11	RTO e RPO come sopra
Indisponibilità della persona chiave	Infrastruttura come codice, runbook scritti, accesso di emergenza con un depositario (documento 11); deposito del codice: Percorso R09	–
Cessazione o insolvenza di Trailgun	Esportazione garantita e assistenza all'uscita (piano di uscita, documento 56); deposito del codice con rilascio in caso di insolvenza o cessazione senza subentro: Percorso R09 e documento 57	sezione 14.4

14.4 Uscita e portabilità

a) Alla cessazione: 30 giorni di accesso in sola lettura con esportazione; poi cancellazione di tutti i dati dello studio entro i 30 giorni successivi, compresi testi estratti, cache OCR, conversazioni con gli agenti, indici, registri delle lavorazioni e utenti, con conferma scritta entro 5 giorni lavorativi (certificato di cancellazione, documento 54). Le copie escono per rotazione nei 14 giorni successivi: al massimo 74 giorni dalla cessazione, salvo obblighi di legge. I dati di fatturazione dello studio si conservano 10 anni (art. 2220 c.c.). Procedura 28.

b) Formato: archivio ZIP cifrato con documenti originali, elaborati in DOCX e PDF/A, testi in TXT, dati strutturati in JSON e CSV, registro delle attività e log degli accessi penali in CSV, indice dei file con impronte SHA-256; consegna con link temporaneo cifrato o via API, entro 10 giorni lavorativi dalla richiesta, con estrazione assistita da Trailgun e certificato di restituzione (documento 53). L'esportazione complessiva in autonomia dall'app è la tappa R02 del Percorso.

c) Assistenza all'uscita: 30 giorni inclusi nel canone; per i clienti DORA o equiparati fino a 12 mesi alle condizioni economiche in vigore, con continuità del servizio e collaborazione al trasferimento (art. 30, par. 3, lett. f, DORA). Piano di uscita e di transizione: documento 56.

SEZIONE 15

Gestione degli incidenti

Sintesi della procedura 25 (risposta agli incidenti) e 26 (violazioni dei dati). Artt. 17-19 DORA; Reg. delegati (UE) 2024/1772 e 2025/301, Reg. di esecuzione (UE) 2025/302; art. 33 GDPR.

15.1 Il processo

1. **Rilevazione**: allarmi e sonda esterna, GuardDuty, segnalazioni di clienti, utenti, fornitori, ricercatori e personale, a security@trailgun.ai o al numero di reperibilità.
2. **Valutazione e classificazione** su tre livelli (grave, significativo, minore), allineati ai criteri del Reg. delegato (UE) 2024/1772: clienti colpiti, durata e inattività, perdita di dati, criticità dei servizi, diffusione, impatto economico.
3. **Contenimento, eliminazione della causa, ripristino**, con la conservazione delle evidenze (log di sicurezza a 12 mesi).
4. **Comunicazione** al Cliente nei tempi della tabella 15.2, con i modelli di notifica del documento 51.
5. **Revisione dopo l'incidente**: cause, azioni correttive, aggiornamento dei controlli, del Registro dei rischi ICT e di questo documento.
6. **Registro** degli incidenti e delle violazioni dei dati personali, con estratto al Titolare su richiesta IN ESSERE.

15.2 Tempi di comunicazione al Cliente

Impegni contrattuali dalla firma. Decorrono da quando Trailgun viene a conoscenza dell'incidente.

COMUNICAZIONE	ENTRO	CONTENUTO E MODALITÀ
Notifica iniziale di un incidente TIC che incide o può incidere sul servizio o sui dati del Cliente	**2 ore**	Email al contatto di sicurezza del Cliente e telefono al referente, con le informazioni disponibili

COMUNICAZIONE	ENTRO	CONTENUTO E MODALITÀ
Aggiornamenti	ogni 24 ore	Fino alla chiusura, e a ogni cambiamento rilevante
Relazione intermedia	48 ore dalla notifica iniziale	Dati per la classificazione e per i modelli di segnalazione del Cliente (Reg. 2025/302), compresa l'origine presso Trailgun o un suo fornitore
Relazione finale	20 giorni dalla chiusura	Cause, impatti, durata, dati coinvolti, azioni correttive; in ogni caso in tempo per la relazione finale del Cliente entro un mese
Minacce informatiche significative	24 ore	Minacce che possono riguardare il Cliente (art. 19, par. 2, DORA)
Violazione dei dati personali	24 ore	Senza ingiustificato ritardo; natura, categorie e numero approssimativo di interessati e registrazioni, conseguenze, misure, contatto (art. 33, par. 3, GDPR), anche per fasi (par. 4); per il Titolare soggetto a DORA vale anche la notifica di 2 ore

15.3 Perché questi tempi

Un'entità soggetta a DORA invia all'autorità la notifica iniziale di un incidente grave entro 4 ore dalla classificazione e comunque entro 24 ore dalla conoscenza, la relazione intermedia entro 72 ore dalla notifica iniziale e la finale entro un mese dall'ultima intermedia (Reg. delegato (UE) 2025/301, art. 5). Quando sono colpiti servizi critici, un incidente è grave se c'è stato un accesso malevolo non autorizzato riuscito, con possibili perdite di dati, oppure se si superano due o più soglie dei criteri, fra cui l'indisponibilità oltre le 2 ore di un servizio che supporta una funzione essenziale o importante (Reg. delegato (UE) 2024/1772, art. 8). I tempi di Trailgun sono più stretti per lasciare al Cliente il margine di classificare e segnalare. Per i dati personali il GDPR chiede al responsabile di informare il titolare «senza ingiustificato ritardo» (art. 33, par. 2) senza fissare ore: le 24 ore sono un impegno nostro.

15.4 Assistenza e priorità

Trailgun assiste il Cliente in un incidente TIC legato al servizio senza costi aggiuntivi (art. 30, par. 2, lett. f, DORA). Un sospetto incidente sui dati è sempre priorità 1: presa in carico entro 1 ora, 24/7; soluzione o aggiramento entro 4 ore; aggiornamenti ogni 2 ore fino al ripristino.

SEZIONE 16

Sicurezza fisica e ambientale

Trailgun non ha data center né server propri.

16.1 Data center

Tutta l'infrastruttura di produzione sta nei data center AWS della regione eu-central-1, con le copie in eu-west-1. Controlli fisici e ambientali (accessi, sorveglianza, alimentazione, raffreddamento, incendio), smaltimento dei supporti e manutenzione dell'hardware sono di AWS, secondo il modello di responsabilità condivisa, e sono coperti dalle sue certificazioni ISO/IEC 27001, 27017 e 27018, dai rapporti SOC 2 e dall'attestazione C5. I rapporti si ottengono da AWS Artifact e Trailgun li fornisce su richiesta.

16.2 Uffici e dispositivi

Negli uffici di Trailgun non ci sono server né archivi dei dati delle pratiche. I dispositivi del personale seguono la politica P14 (uso accettabile): disco cifrato, blocco dello schermo, aggiornamenti automatici, secondo fattore sugli account di lavoro, nessun dato delle pratiche fuori dalla piattaforma. I dispositivi sono censiti nell'inventario degli asset (documento 42) IN ESSERE.

SEZIONE 17

Personale e formazione

Art. 13, par. 6, e art. 30, par. 2, lett. i, DORA; art. 29 e art. 32, par. 4, GDPR; art. 4 AI Act. Politica P13, procedura 21.

17.1 Riservatezza e designazione

Chi lavora per Trailgun con accesso ai dati firma un impegno scritto di riservatezza e riceve la designazione al trattamento (art. 29 GDPR, art. 2-quaterdecies d.lgs. 196/2003). Gli obblighi sopravvivono alla fine del rapporto IN ESSERE.

17.2 Formazione

Formazione su sicurezza e protezione dei dati all'ingresso e ogni anno per il personale e i collaboratori con accesso; alfabetizzazione sull'IA ogni anno (art. 4 Reg. (UE) 2024/1689), per il personale e, con la sessione di avvio, per gli utenti degli studi. Ogni sessione è nel Registro della formazione (documento 43) IN ESSERE. Trailgun partecipa ai programmi di sensibilizzazione e formazione del Cliente alle condizioni del contratto (art. 30, par. 2, lett. i, DORA).

17.3 Verifiche e cessazione

Verifica dei precedenti per chi accede alla produzione, nei limiti dell'art. 8 della legge 300/1970 e dell'art. 10 GDPR IN ESSERE. Alla cessazione, revoca degli accessi entro 24 ore, rotazione dei segreti a cui la persona aveva accesso, restituzione dei dispositivi e verbale (procedura 21).

SEZIONE 18

Fornitori e catena di fornitura

Chi riceve dati, dove, con quali garanzie. Art. 28, par. 2 e 4, GDPR; artt. 28-30 DORA; Reg. delegato (UE) 2025/532. Politica P10, procedura 29, registro 15.

18.1 Subfornitori

L'elenco completo, con entità, sede, regioni, garanzie di trasferimento, DPA e criticità, è il Registro dei subfornitori (documento 15) ed è pubblicato su https://trailgun.ai/subprocessors.

FORNITORE	SERVIZIO	DATI	LUOGO	GARANZIE
Amazon Web Services	Infrastruttura, conservazione, login (Cognito), email di Cognito (SES), log	Tutti	Germania; copie in Irlanda	DPA di AWS firmato; certificazioni AWS
Amazon Bedrock (AWS)	Modelli Claude di Anthropic per tutti gli agenti; embeddings Amazon Titan	Testo dei documenti, dati estratti, atti, domande	Regioni AWS UE	Servizio AWS: il produttore del modello non riceve i dati; opt-out dei servizi di IA
AWS Textract, Transcribe	OCR, trascrizione	PDF e immagini; registrazioni, anche intercettazioni	Germania	opt-out dei servizi di IA con policy di AWS Organizations
Resend	Email in uscita e risposte in entrata	Indirizzi, testi, allegati delle risposte, email di notifica senza dati delle pratiche	invio e ricezione su AWS in Irlanda; società USA	DPA firmato; Data Privacy Framework verificato; valutazione del trasferimento
Wolters Kluwer Italia (One LEGALE)	Banca dati giuridica	Stringhe di ricerca senza dati delle pratiche	Italia	DPA firmato
Openapi (con Namirial)	Firma qualificata, visure	PDF da firmare, dati del firmatario, P.IVA e C.F. delle imprese	Italia	DPA firmato
DocuPipe (Hoss Inc.)	OCR di riserva, solo per lo studio che lo accende	Singoli file non letti da Textract	USA	DPA firmato; valutazione del trasferimento; opzione spenta di default
Telegram, **Twilio**	Notifiche agli utenti che le scelgono (Telegram; SMS e WhatsApp)	Avviso e link, senza dati delle pratiche	fuori dall'UE	nessun dato delle pratiche
Stripe	Pagamenti dello studio con fatturazione a consumo	Dati di pagamento dello studio	UE e USA	titolare autonomo per i dati di pagamento; nessun dato delle pratiche

FORNITORE	SERVIZIO	DATI	LUOGO	GARANZIE
Microsoft	Login per la revisione in Word	Nessuno dal server: il file va al tenant del Cliente	–	non è un subfornitore
Google Workspace	Caselle delle persone di Trailgun	Email inviate agli indirizzi delle persone	–	non riceve dati dalla piattaforma
GitHub, npm, Docker Hub, Let's Encrypt	Codice e CI, pacchetti, immagini base, certificati	Nessun dato dei clienti	USA	catena di fornitura del software

18.2 Valutazione e contratti

Ogni fornitore si valuta prima dell'ingaggio e ogni anno (procedura 29, Valutazione dei fornitori): sicurezza, certificazioni, regioni, DPA e garanzie di trasferimento, valutazione d'impatto del trasferimento quando serve, sostituibilità e uscita, concentrazione. L'esito sta nel Registro dei subfornitori (documento 15). I DPA con AWS, Resend, DocuPipe, Openapi e Wolters Kluwer sono firmati e archiviati; le valutazioni dei trasferimenti verso Resend e DocuPipe sono svolte e si mostrano in audit IN ESSERE. Per AWS e per gli altri fornitori a condizioni standard, i diritti di verifica si esercitano sui loro rapporti di audit e certificazione.

18.3 Modifiche ai subfornitori

Preavviso di 30 giorni per email all'amministratore e al DPO del Cliente, con identità, attività, luogo e garanzie; 60 giorni per i clienti DORA con funzioni essenziali o importanti, e in quel caso il cambiamento non si attua prima della scadenza né finché l'opposizione è pendente (Reg. delegato (UE) 2025/532, art. 5). Il Cliente può opporsi entro il preavviso; se l'opposizione non si risolve in 30 giorni, può recedere senza penali con il rimborso della quota pagata e non goduta. Una sostituzione urgente, solo per sicurezza o cessazione del fornitore, si comunica entro 72 ore e lascia il diritto di opposizione. L'elenco aggiornato è allegato al DPA (documento 07, Allegato 3) e pubblicato su https://trailgun.ai/subprocessors.

18.4 Concentrazione

Amazon Web Services EMEA SARL è fra i fornitori terzi critici designati dalle Autorità europee di vigilanza il 18/11/2025. Con i modelli su Amazon Bedrock la quasi totalità del trattamento sta su AWS: un solo fornitore principale, già presente nel registro delle informazioni di molti clienti e sotto la sorveglianza diretta delle autorità europee. Il Cliente lo pesa nella valutazione dell'art. 29 DORA. Trailgun non è un fornitore critico ai sensi dell'art. 31 DORA: è sotto i criteri dell'art. 31, par. 2, e del Reg. delegato (UE) 2024/1502.

18.5 Catena di fornitura del software

Pacchetti e immagini arrivano da npm, Docker Hub e GitHub. Dependabot e la scansione delle immagini li controllano; le immagini base di Node.js e di Caddy sono fissate a una versione; la scansione dei segreti copre l'intero repository. Nessuno di questi fornitori riceve dati dei clienti.

SEZIONE 19

Fascicoli penali

Dati relativi a reati (art. 10 GDPR, art. 2-octies d.lgs. 196/2003), intercettazioni e registrazioni: un regime più stretto. Politica P16.

19.1 Come si riconosce un fascicolo penale

La materia del fascicolo (penale, civile, amministrativo, tributario) la sceglie l'avvocato nel modulo, prima di caricare l'archivio. Senza quella scelta (API, caselle, lotti) la stabilisce un classificatore della natura del fascicolo, che ne ricava anche gli estremi del procedimento.

19.2 Le misure in essere

- Nessun indice di embeddings sui fascicoli penali o misti: il testo non va al servizio di embeddings IN ESSERE.
- Registro degli accessi: ogni consultazione (una all'ora per utente), domanda, analisi, confronto fra depositi, timeline, grafo delle relazioni e scheda dell'imputato si annota nel registro delle attività, consultabile ed esportabile dal Titolare e conservato per tutta la durata del contratto IN ESSERE.
- Ogni uscita delle funzioni sul fascicolo è una segnalazione con la sua fonte, mai una conclusione IN ESSERE.
- Audio e intercettazioni trascritti con Amazon Transcribe in eu-central-1 IN ESSERE.

19.3 Dove va il testo

a) Il testo dei fascicoli penali si elabora solo su Amazon Bedrock nella regione UE: il produttore del modello non lo riceve e AWS non lo usa per migliorare i propri servizi IN ESSERE.

b) Textract e Transcribe sono esclusi dal miglioramento dei servizi di IA di AWS con la policy dell'organizzazione IN ESSERE.

c) La riserva DocuPipe è spenta di default: lo studio che tratta fascicoli penali la lascia spenta, e i file che Textract non legge restano da trattare a mano IN ESSERE.

d) Le notifiche esterne non portano dati delle pratiche, nemmeno il titolo dell'atto IN ESSERE.

19.4 Ruoli

Il titolare è lo studio, che tratta i dati relativi a reati per la difesa in giudizio (art. 2-octies, comma 3, lett. e, d.lgs. 196/2003) e svolge la valutazione d'impatto quando il trattamento è su larga scala (art. 35, par. 3, lett. b, GDPR). Trailgun la assiste con le informazioni necessarie entro 10 giorni lavorativi dalla richiesta e con il modello precompilato del documento 50.

SEZIONE 20

Sicurezza dell'intelligenza artificiale

Che cosa può andare storto con un sistema di agenti su documenti non fidati, e come lo contiamo. Politica P15, documento 09.

20.1 I modelli e chi li sceglie

Tutti gli agenti usano Claude Opus 5.5 di Anthropic su Amazon Bedrock nelle regioni dell'Unione. La scelta dei modelli, l'ampiezza della ricerca e il motore OCR sono impostazioni solo della piattaforma: studi e utenti non li vedono e non li cambiano. I prompt stanno in un registro centrale; il loro testo si legge e si cambia solo dal backoffice della piattaforma e non arriva mai al browser di uno studio, che vede di ogni prompt una sintesi e può solo accodare testi propri IN ESSERE.

20.2 Isolamento dei dati nelle chiamate ai modelli

Ogni chiamata è composta dal codice con i documenti e i dati della pratica su cui si lavora, i materiali e le regole dello studio e le fonti giuridiche scaricate. Gli strumenti dell'assistente dell'atto sono legati all'atto della conversazione: atto e utente arrivano dal contesto della richiesta composto dal server, mai dagli argomenti scelti dal modello, e ogni strumento ripassa dal controllo di visibilità. Solo su richiesta dell'utente l'assistente allinea a una regola le altre pratiche dello stesso lotto, senza rifarle. L'analisi del faldone nella modalità estesa usa la cache dei prompt di Bedrock, nella stessa regione, per un'ora, per non ripagare la lettura dello stesso faldone. Le conversazioni dell'assistente dell'atto si conservano nell'archivio di Trailgun e si cancellano con la pratica (sezione 4.5). La funzione unica che chiama i modelli registra modello, agente, token e costo, mai il testo IN ESSERE.

20.3 Addestramento

Né Trailgun né chi esegue i modelli addestra sui dati dei clienti. Trailgun usa modelli di terzi senza addestrarli né ottimizzarli e non usa i dati delle pratiche per finalità proprie. Su Amazon Bedrock i dati restano nella regione, AWS non li usa per addestrare i modelli e non li condivide con il produttore del modello; la policy di AWS Organizations esclude anche i contenuti di Textract e Transcribe dal miglioramento dei servizi di IA di AWS IN ESSERE. La dichiarazione firmata è il documento 60.

20.4 Minacce e contromisure

MINACCIA	CONTROMISURA	STATO
Istruzioni nascoste nei documenti (prompt injection indiretta)	Il testo dei documenti arriva al modello fra delimitatori espliciti e il prompt dichiara che è un dato da analizzare, mai un ordine. Il segnaposto del testo è obbligatorio nel registro: una versione del prompt che lo dimentica non si salva. Le uscite degli agenti seguono schemi strutturati	IN ESSERE
Azioni verso l'esterno indotte da un documento	Di default le comunicazioni ai clienti dello studio e alle controparti le prepara un agente e le approva l'avvocato; la modalità automatica la sceglie lo studio, e la mail lo dichiara. Il testo dell'atto si scrive da un solo punto del codice, con versioni. Le regole di memoria si salvano solo dopo conferma dell'utente, e valgono per lo studio solo con l'approvazione di un amministratore	IN ESSERE
Dati inventati	Ogni dato dell'atto viene da un documento, con la fonte, oppure è «N/D»; i riferimenti a documento e pagina dell'analisi del faldone sono verificati in codice; controlli di coerenza e conteggi; verifica giurisprudenziale su banca dati, attivabile	IN ESSERE

MINACCIA	CONTROMISURA	STATO
Decisioni senza persona	Gli elaborati sono bozze: solo un utente autorizzato conferma l'atto, firma e deposito restano all'avvocato; nessuna decisione automatizzata sulle persone (art. 22 GDPR)	IN ESSERE
Fuga di dati verso la banca dati giuridica	Regola in codice, con test, che toglie nomi, codici fiscali, importi e dati delle pratiche dalle stringhe di ricerca prima che partano	IN ESSERE
Riuso dei dati da parte del fornitore del modello	Modelli ed embeddings su Amazon Bedrock UE; regioni fuori dall'Unione rifiutate dal codice	IN ESSERE
Riuso dei contenuti da parte dei servizi di IA di AWS	Esclusione con una policy di AWS Organizations per Textract, Transcribe e Bedrock	IN ESSERE
Uso degli strumenti per raggiungere altri dati	Atto e utente degli strumenti fissati dal server, non dal modello; controllo di visibilità a ogni chiamata	IN ESSERE
Fuga fra studi	Predicato unico di visibilità, indici nella cartella della pratica, cache OCR e del layout per studio	IN ESSERE

20.5 Trasparenza

I DOCX e i PDF prodotti dagli agenti, compreso il PDF della revisione in Word, portano metadati leggibili da macchina: la descrizione «AI-generated, EU AI Act art. 50», le parole chiave e il tipo di fonte digitale IPTC dei contenuti generati da un modello (art. 50, par. 2, Reg. (UE) 2024/1689). Le copie dei documenti del cliente e le fatture non si marcano. Le chat dell'assistente dell'atto e dell'assistenza dicono all'utente che sta interagendo con un assistente di IA; la pagina dell'atto indica che la bozza è generata con l'IA e va rivista dall'avvocato; le mail della modalità automatica lo dichiarano al destinatario (art. 50, par. 1) IN ESSERE.

20.6 Classificazione

Nella destinazione d'uso dichiarata (studi, servicer, banche) Trailgun non è un sistema ad alto rischio: il punto 8, lett. a, dell'Allegato III riguarda i sistemi usati da un'autorità giudiziaria o per suo conto, e la vendita a uffici giudiziari è esclusa. Se l'uso cambiasse, gli obblighi per l'alto rischio dell'Allegato III si applicherebbero dal 02/12/2027. Anthropic, fornitore del modello per finalità generali, ha firmato il codice di buone pratiche per i modelli GPAI. La dichiarazione completa è nel documento 09, AI Act e uso dell'IA nella professione.

SEZIONE 21

Test, verifiche e audit

Artt. 24-26 DORA; art. 30, par. 3, lett. d ed e, DORA; art. 32, par. 1, lett. d, GDPR.

21.1 Programma dei test

TEST	FREQUENZA E MODALITÀ	STATO
Test automatici	A ogni rilascio: tipi, unitari, end-to-end, isolamento fra studi	IN ESSERE
Scansione dei segreti	A ogni verifica, su tutta la storia del repository (gitleaks)	IN ESSERE
Scansione delle dipendenze e delle immagini	Settimanale (Dependabot) e a ogni immagine (ECR)	IN ESSERE
Prova automatica di ripristino	A ogni verifica della CI: copie del database e del volume ripristinate e verificate	IN ESSERE
Prova di ripristino sullo snapshot reale	Trimestrale, in ambiente isolato, con integrità e RTO misurati e verbale	IN ESSERE
Prova del piano di continuità	Annuale, con esercitazione sugli scenari del documento 11	IN ESSERE
Scansione esterna dell'applicazione	Mensile	PERCORSO R05
Penetration test	Annuale, da un terzo indipendente, e dopo ogni cambiamento rilevante dell'architettura; sintesi e piano di rimedio al Cliente sotto riservatezza	PERCORSO R06

TEST	FREQUENZA E MODALITÀ	STATO
Prova di ripristino regionale	Annuale	PERCORSO R10

21.2 Test guidati dalla minaccia

Trailgun partecipa ai test di penetrazione guidati dalla minaccia (TLPT) del Cliente, alle condizioni concordate per non mettere a rischio gli altri clienti, anche nella forma congiunta prevista dall'art. 26, par. 4, DORA. Il TLPT riguarda le entità individuate dall'autorità; non si applica agli intermediari 106 (art. 6 d.lgs. 23/2025, che non richiama gli artt. 26-27 DORA).

21.3 Audit del Cliente e delle autorità

La richiesta si fa con il modulo del documento 52.

TIPO	CONDIZIONI
Ordinario	Uno all'anno, preavviso di 30 giorni, in orario lavorativo, fino a 2 giorni in loco, senza compromettere gli altri clienti; prima i documenti e le certificazioni disponibili
Straordinario	Dopo un incidente grave o su richiesta di un'autorità, con preavviso di 5 giorni lavorativi
DORA, funzioni essenziali o importanti, e autorità	Accesso, ispezione, audit e copia della documentazione illimitati (art. 30, par. 3, lett. e, DORA; art. 8 d.lgs. 23/2025), anche congiunti
Questionari	Risposta entro 15 giorni lavorativi; uno all'anno senza costi, oltre su accordo
Costi	Ciascuna parte sostiene i propri

21.4 Cooperazione con le autorità

Trailgun coopera pienamente con le autorità competenti del Cliente e con le persone da esse nominate (art. 30, par. 2, lett. g, DORA). La Banca d'Italia può effettuare accessi e ispezioni presso i fornitori TIC a supporto di funzioni essenziali o importanti e convocarne amministratori e personale (art. 8 d.lgs. 23/2025); l'omessa collaborazione è sanzionata anche in capo al fornitore (art. 144, comma 8-bis, TUB).

SEZIONE 22

Certificazioni, assicurazioni e percorso

Che cosa è certificato oggi, come è coperto il rischio residuo e dove sono le tappe successive.

Le certificazioni che coprono il servizio sono quelle di AWS per l'infrastruttura: ISO/IEC 27001, 27017 e 27018, SOC 2 e C5, con i rapporti da AWS Artifact su richiesta. Le tappe del Percorso di certificazione e piattaforma, con date, evidenze attese e modo in cui il Cliente ne è informato, sono nel documento 12: R01-R17, dal primo penetration test (R06) al certificato ISO/IEC 27001:2022 (R16).

22.1 Assicurazioni

Polizza cyber per [€ ...] per sinistro e per anno e polizza di responsabilità civile professionale per errori e omissioni del software per [€ ...] per sinistro e per anno, con [compagnia] IN ESSERE; certificato al Cliente su richiesta.

22.2 Deposito del codice

Il deposito del codice sorgente e delle istruzioni di ricostruzione presso un agente terzo, aggiornato ogni trimestre e rilasciato al Cliente in caso di insolvenza o cessazione dell'attività o del servizio senza subentro, è la tappa R09 del Percorso; le condizioni sono nel term sheet del documento 57. Fino ad allora la continuità del Cliente è tutelata dall'esportazione completa dei dati e dall'assistenza all'uscita (sezione 14.4).

ALLEGATO A

Elenco dei controlli

Ogni controllo con il suo stato al 01/12/2026. Riferimenti: controlli dell'Allegato A di ISO/IEC 27001:2022 e articoli di DORA o del Reg. delegato (UE) 2024/1774 («RTS»). Gli stessi controlli, con l'evidenza, sono nella dichiarazione di applicabilità (documento 14).

ID	CONTROLLO	STATO	RIF.
GV-01	Responsabile della sicurezza nominato (CEO)	IN ESSERE	5.2 · art. 5 DORA
GV-02	Responsabile della sicurezza dedicato	PERCORSO R13	5.2, 5.3
GV-03	Caselle security@ e privacy@ presidiate; DPO nominato e comunicato al Garante	IN ESSERE	5.5 · art. 37 GDPR
GV-04	Politiche P01-P17 e procedure 20-31 adottate dall'organo amministrativo	IN ESSERE	5.1, 5.37
GV-05	Registro dei rischi ICT con metodo, titolari e trattamento	IN ESSERE	5.1 · art. 6 DORA
GV-06	SGSI definitivo e certificato ISO/IEC 27001:2022	PERCORSO R08, R16	art. 28(5) DORA
GV-07	Infrastruttura descritta come codice e ricostruibile	IN ESSERE	8.9
GV-08	Account AWS dedicato e intestato a Trailgun, in AWS Organizations	IN ESSERE	5.23
GV-09	Politica di segnalazione responsabile pubblicata, security.txt	IN ESSERE	5.5, 8.8
TI-01	Predicato unico di visibilità per ogni interrogazione su dati di un cliente	IN ESSERE	5.15, 8.3
TI-02	Test automatici sull'isolamento fra studi a ogni rilascio	IN ESSERE	8.29
TI-03	Visibilità per cliente: studio, privato, selezionati	IN ESSERE	5.15
TI-04	Cache OCR e del layout per studio, cancellate con la pratica	IN ESSERE	8.10
TI-05	Ambienti non di produzione con pool, dati e servizi propri	IN ESSERE	8.31
AC-01	Login su invito con Amazon Cognito, protocollo SRP	IN ESSERE	5.16, 5.17
AC-02	Secondo fattore TOTP obbligatorio per tutti gli utenti	IN ESSERE	8.5 · art. 9(4)(d) DORA
AC-03	Politica delle password: almeno 10 caratteri, maiuscole, minuscole, cifre	IN ESSERE	5.17
AC-04	Verifica del token d'identità a ogni richiesta	IN ESSERE	8.5
AC-05	Ruoli admin e membro; permessi per membro	IN ESSERE	5.15, 5.18
AC-06	Ruoli operator e viewer imposti dal server	IN ESSERE	5.15, 8.2
AC-07	Chiavi API: solo impronta SHA-256, revoca, 120 richieste al minuto	IN ESSERE	5.17, 8.5
AC-08	Webhook in entrata verificati, in uscita firmati	IN ESSERE	8.5, 8.24
AC-09	Nessun SSH; amministrazione con Systems Manager	IN ESSERE	8.2, 8.20
AC-10	Ruolo dell'istanza a privilegi limitati	IN ESSERE	8.2 · art. 9(4)(c) DORA
AC-11	CI con OIDC, un ruolo per ambiente limitato al proprio branch	IN ESSERE	8.2, 8.4
AC-12	Secondo fattore su AWS (root, Identity Center e console) e console dei fornitori	IN ESSERE	8.5 · art. 21 RTS
AC-13	Credenziali amministrative temporanee (IAM Identity Center); 2FA obbligatoria su GitHub	IN ESSERE	8.2, 8.5
AC-14	Registro degli accessi del personale ai contenuti	IN ESSERE	8.15, 8.2

ID	CONTROLLO	STATO	RIF.
AC-15	Revisione trimestrale degli accessi privilegiati (modello 44)	IN ESSERE	5.18
AC-16	Revoca degli accessi entro 24 ore dalla cessazione	IN ESSERE	5.18, 6.5
CR-01	Cifratura AES-256 dei dischi, degli snapshot e delle copie (AWS KMS)	IN ESSERE	8.24 · art. 6 RTS
CR-02	Bucket temporaneo cifrato, pubblico bloccato, solo TLS, scadenza 1 giorno	IN ESSERE	8.24, 8.10
CR-03	HTTPS con TLS 1.2-1.3, certificati automatici, redirect	IN ESSERE	8.24, 8.20
CR-04	HSTS di un anno	IN ESSERE	8.26
CR-05	Segreti in Parameter Store, mai nel codice o nell'immagine; scansione gitleaks	IN ESSERE	5.17, 8.24
CR-06	Rotazione dei segreti dei fornitori ogni 12 mesi	IN ESSERE	8.24
CR-07	Chiavi KMS gestite da Trailgun per database e file	PERCORSO R12	8.24
NW-01	In ingresso solo TCP 80, TCP 443, UDP 443	IN ESSERE	8.20, 8.22
NW-02	IMDSv2 obbligatorio, AMI fissata	IN ESSERE	8.9
NW-03	Intestazioni di sicurezza (CSP, X-Content-Type-Options, Referrer-Policy, frame-ancestors)	IN ESSERE	8.26
NW-04	Limiti sugli archivi caricati (voci e dimensione)	IN ESSERE	8.7, 8.26
NW-05	Bilanciatore con AWS WAF, più zone di disponibilità	PERCORSO R12	8.20, 8.14
SD-01	Verifica obbligatoria prima di ogni rilascio, anche manuale: tipi, unitari, end-to-end, segreti, ripristino	IN ESSERE	8.25, 8.29 · art. 9(4)(e) DORA
SD-02	Rilascio rifiutato con lavorazioni in corso; produzione solo dal branch pulito	IN ESSERE	8.32
SD-03	Snapshot prima di ogni rilascio; copia del database prima delle migrazioni	IN ESSERE	8.32, 8.13
SD-04	Migrazioni numerate, solo in avanti, compatibili con l'immagine precedente	IN ESSERE	8.32
SD-05	Novità come opzioni spente; scelta congelata sull'atto	IN ESSERE	8.32
SD-06	Protezione dei branch di ambiente e richiesta di integrazione obbligatoria	IN ESSERE	8.4, 8.32
SD-07	Container non root; immagine di Caddy fissata	IN ESSERE	8.9
SD-08	Registro dei cambiamenti di produzione (documento 45)	IN ESSERE	8.32
VM-01	Dependabot settimanale su pacchetti, immagini e Actions	IN ESSERE	8.8 · art. 10 RTS
VM-02	Scansione delle immagini a ogni caricamento su ECR	IN ESSERE	8.8
VM-03	Tempi di correzione 72 ore, 7, 30, 90 giorni	IN ESSERE	8.8 · art. 9(4)(f) DORA
VM-04	Aggiornamenti mensili di sicurezza del sistema operativo dell'host	IN ESSERE	8.8
VM-05	Scansione esterna mensile dell'applicazione	PERCORSO R05	8.8 · art. 25 DORA
LM-01	Log di accesso HTTP e applicativi su CloudWatch a 90 giorni	IN ESSERE	8.15 · art. 12 RTS
LM-02	Log applicativi senza testo dei documenti né segreti	IN ESSERE	8.11, 8.15
LM-03	CloudTrail su tutte le regioni con convalida, GuardDuty, sessioni SSM, log di sicurezza a 12 mesi	IN ESSERE	8.15, 8.16 · art. 10 DORA
LM-04	Sonda esterna ogni minuto e allarmi 24/7	IN ESSERE	8.16
LM-05	Registro delle attività dello studio, esportabile	IN ESSERE	8.15

ID	CONTROLLO	STATO	RIF.
LM-06	Versioni dell'atto con autore e motivo	IN ESSERE	8.15
LM-07	Eventi di costo senza testo dei documenti	IN ESSERE	8.11, 8.12
LM-08	Sincronizzazione degli orologi (Amazon Time Sync)	IN ESSERE	8.17
BR-01	Snapshot giornaliero, 14 conservati	IN ESSERE	8.13 · art. 12 DORA
BR-02	Copia cifrata in Irlanda, 14 giorni	IN ESSERE	8.13, 8.14
BR-03	Scadenza a 14 giorni degli snapshot prima del rilascio	IN ESSERE	8.10, 8.13
BR-04	Prova di ripristino trimestrale sullo snapshot reale, con verbale; prova automatica nella CI	IN ESSERE	8.13 · art. 12(2) DORA
BR-05	Snapshot ogni 4 ore	PERCORSO R01	8.13
BR-06	Procedura di ripristino regionale scritta e provata	PERCORSO R03	5.30
BR-07	Copie protette dalla cancellazione per 7 giorni	PERCORSO R11	8.13
BC-01	Piano di continuità operativa e ripristino adottato, provato ogni anno	IN ESSERE	5.29, 5.30 · art. 11 DORA
BC-02	Prova regionale annuale	PERCORSO R10	5.30 · art. 11(6) DORA
BC-03	Cancellazione completa a fine contratto, con strumento e conferma	IN ESSERE	8.10 · art. 30(2)(d) DORA
BC-04	Esportazione complessiva nei formati dichiarati, entro 10 giorni lavorativi	IN ESSERE	5.23 · art. 28(8) DORA
BC-05	Deposito del codice presso un agente terzo	PERCORSO R09	5.30
IM-01	Notifica iniziale 2 ore, intermedia 48 ore, finale 20 giorni; violazioni 24 ore	IN ESSERE	5.24, 5.26 · art. 30(3)(b) DORA
IM-02	Classificazione su 3 livelli e registro degli incidenti e delle violazioni	IN ESSERE	5.25, 5.27 · art. 17 DORA
PS-01	Infrastruttura in data center AWS certificati	IN ESSERE	7.1-7.14 (AWS)
HR-01	Impegno di riservatezza e designazione al trattamento	IN ESSERE	6.6
HR-02	Formazione su sicurezza, privacy e IA all'ingresso e ogni anno (registro 43)	IN ESSERE	6.3 · art. 13(6) DORA
HR-03	Verifica dei precedenti per l'accesso alla produzione	IN ESSERE	6.1
SP-01	Registro e valutazione annuale dei fornitori (registro 15, procedura 29)	IN ESSERE	5.19, 5.22
SP-02	DPA firmati con i subfornitori; valutazioni dei trasferimenti	IN ESSERE	5.20 · art. 28(4) GDPR
SP-03	DocuPipe come opzione dello studio spenta di default	IN ESSERE	5.19
SP-04	Notifiche esterne senza dati delle pratiche	IN ESSERE	5.14, 8.12
SP-05	Elenco dei subfornitori pubblicato su https://trailgun.ai/subprocessors	IN ESSERE	5.20
PF-01	Fascicoli penali: nessun indice di embeddings	IN ESSERE	5.34, 8.11
PF-02	Fascicoli penali: registro di consultazioni, domande, analisi, timeline, grafi e schede	IN ESSERE	8.15, 5.34
AI-01	Documenti fra delimitatori e dichiarati dati; segnaposto obbligatorio nel registro dei prompt	IN ESSERE	8.28
AI-02	Prompt e scelta dei modelli solo della piattaforma	IN ESSERE	8.2, 5.15
AI-03	Fonte per ogni dato o «N/D»; riferimenti verificati in codice	IN ESSERE	8.28
AI-04	Comunicazioni esterne approvate dall'avvocato di default	IN ESSERE	5.15

ID	CONTROLLO	STATO	RIF.
AI-05	Modelli ed embeddings su Amazon Bedrock UE; regioni fuori dall'UE rifiutate dal codice	IN ESSERE	5.23 · art. 28 GDPR
AI-06	Esclusione dei contenuti dal miglioramento dei servizi di IA di AWS	IN ESSERE	5.23
AI-07	Filtro dei dati delle pratiche nelle ricerche su One LEGALE, con test	IN ESSERE	8.11, 8.12
AI-08	Marcatura «AI-generated» in DOCX e PDF; avviso di IA nelle chat, sulla pagina dell'atto e nelle mail automatiche	IN ESSERE	art. 50 AI Act
TS-01	Primo penetration test indipendente, poi annuale	PERCORSO R06	8.8, 5.35 · art. 24-25 DORA

ALLEGATO B

Politiche, procedure e registri

Dove ogni area di questo documento è governata e dove sta la sua evidenza. Le tappe successive sono nel documento 12.

AREA	POLITICA	PROCEDURA	REGISTRO O MODELLO
Governance e rischio (sezioni 2, 3)	P01, P02	–	41 Registro dei rischi ICT; 14 Dichiarazione di applicabilità
Asset e classificazione (sezione 4)	P11	–	42 Inventario degli asset
Accessi (sezione 7)	P03	21 Ingresso e uscita del personale; 22 Revisione degli accessi	44 Revisione degli accessi
Cifratura e segreti (sezione 8)	P04	23 Gestione delle chiavi e dei segreti	inventario dei segreti
Sviluppo e cambiamenti (sezione 10)	P05, P06	20 Gestione dei cambiamenti	45 Registro dei cambiamenti
Vulnerabilità (sezione 11)	P07	24 Vulnerabilità e segnalazione responsabile	registro delle vulnerabilità
Log e monitoraggio (sezione 12)	P08	25 Risposta agli incidenti	registro degli incidenti
Backup e continuità (sezioni 13, 14)	P09	30 Backup e ripristino; 31 Programma di prova di disaster recovery	verbali delle prove; documento 11
Incidenti e violazioni (sezione 15)	P08	25 Risposta agli incidenti; 26 Violazioni dei dati personali	51 Modelli di notifica; registro delle violazioni
Personale (sezioni 16, 17)	P13, P14, P17	21 Ingresso e uscita del personale	43 Registro della formazione
Fornitori (sezione 18)	P10	29 Valutazione dei fornitori	15 Registro dei subfornitori
Dati personali e uscita (sezioni 14.4, 19)	P12, P16	26, 27 Richieste degli interessati; 28 Restituzione e cancellazione	40 Registro dei trattamenti; 53, 54 Certificati
Intelligenza artificiale (sezione 20)	P15	–	47 Mappa AI Act; documento 09

ALLEGATO C

Corrispondenze normative

Dove questo documento risponde alle norme che le banche e gli intermediari ci chiedono di verificare. Le mappe di dettaglio sono i documenti 17 (DORA), 46 (GDPR art. 28), 47 (AI Act) e 48 (linee guida EBA).

NORMA	TEMA	SEZIONI
DORA art. 9, par. 4, lett. a, c, d, e, f	Politica di sicurezza, accessi, autenticazione forte e cifratura, cambiamenti, patch	2.6, 7, 8, 10, 11
DORA art. 10	Rilevazione delle anomalie	12
DORA art. 11 e art. 12	Continuità; backup, ripristino, RTO e RPO	13, 14
DORA art. 13, par. 6	Formazione, anche con i fornitori	17.2
DORA artt. 17-19	Gestione, classificazione e segnalazione degli incidenti	15
DORA artt. 24-26	Test, compreso il TLPT	21
DORA art. 28, par. 4 e 5	Due diligence; norme adeguate di sicurezza	1, 3
DORA art. 28, par. 8; art. 30, par. 3, lett. f	Strategia e periodo di transizione all'uscita	14.4
DORA art. 29	Concentrazione e subappalto	18.4
DORA art. 30, par. 2, lett. a, b, c, d, f, g, i	Descrizione, luoghi, sicurezza dei dati, restituzione, assistenza negli incidenti, cooperazione con le autorità, formazione	4, 5, 8, 14.4, 15.4, 21.4, 17.2
DORA art. 30, par. 3, lett. a, b, c, d, e	Livelli di servizio, notifiche, piani di emergenza, TLPT, audit illimitati	14.2, 15.2, 14.1, 21.2, 21.3
Reg. delegato (UE) 2024/1774, artt. 6, 10, 12, 20-21	Cifratura, vulnerabilità, log, identità e autenticazione forte	7, 8, 11, 12
Reg. delegato (UE) 2024/1774, artt. 28-41	Quadro semplificato degli intermediari 106	2, 7-14
Reg. delegato (UE) 2025/532, artt. 4-5	Subappalto e modifiche rilevanti	18.2, 18.3
D.lgs. 23/2025, artt. 6 e 8	Regole per gli intermediari 106; ispezioni presso i fornitori	21.2, 21.4
GDPR art. 28, par. 3, lett. c e h	Misure dell'art. 32; informazioni e audit	tutto il documento; 21.3
GDPR art. 32, par. 1, lett. a-d	Cifratura; riservatezza, integrità, disponibilità e resilienza; ripristino; verifica periodica	8, 6-12, 13, 21
GDPR art. 33, par. 2-4	Violazioni dei dati personali	15.2
D.lgs. 196/2003, art. 2-octies; GDPR art. 10	Dati relativi a reati	19
Reg. (UE) 2024/1689, artt. 4 e 50	Alfabetizzazione; trasparenza e marcatura	17.2, 20.5

Questo documento descrive le misure tecniche e organizzative in essere al 01/12/2026. Gli obblighi contrattuali sono quelli del Contratto di servizio, dell'Accordo sul trattamento dei dati (documento 07), dell'Allegato DORA (documento 18) e dell'Accordo sul livello di servizio (documento 55), che riportano gli stessi valori. Le tappe successive sono vincolanti nei termini del documento 12. Le norme sono citate nel testo vigente al 01/12/2026.

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
privacy@trailgun.ai

SITO
trailgun.ai

Segnalazioni di vulnerabilità: https://trailgun.ai/security. Subfornitori: https://trailgun.ai/subprocessors. Il pacchetto di conformità comprende anche i documenti su protezione dei dati, DORA, AI Act, l'Accordo sul trattamento dei dati, le politiche, le procedure, i registri e i questionari: l'indice completo è nel Trust Center (documento 00).