Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO 12

VERSIONE 2.0 · DICEMBRE 2026

Percorso di certificazione e piattaforma

La certificazione ISO/IEC 27001, il primo penetration test indipendente, il deposito del codice, la nuova piattaforma su più zone e i livelli di servizio che ne seguono. Che cosa cambia per il Cliente a ogni tappa, quale evidenza riceve e come ne viene informato.

PRIMA TAPPA	PENETRATION TEST	NUOVA PIATTAFORMA	ISO/IEC 27001
15/12/2026	29/01/2027	30/06/2027	17/12/2027

PREMESSA

Il punto di partenza è già una piattaforma in ordine

Questo è l'unico documento del Pacchetto di conformità che contiene date future. Tutto ciò che gli altri documenti descrivono è in essere alla data di questa versione, 01/12/2026; qui stanno soltanto i passi che portano Trailgun oltre: verifiche indipendenti, certificazione, più zone di disponibilità, livelli di servizio più alti.

CODICE	TITOLARE	APPROVATO DA	VERSIONE
Documento 12	Franco Puppo, CEO e responsabile della sicurezza	Organo amministrativo, [data]	2.0 · stato al 01/12/2026

REVISIONE	DESTINATARI
a ogni tappa completata e almeno ogni trimestre	ICT risk, vendor risk, audit

DOCUMENTI COLLEGATI

00 Trust Center · 05 Sicurezza delle informazioni · 08 DORA · 11 Continuità e incidenti · 14 Dichiarazione di applicabilità · 18 Allegato DORA al contratto · 55 Accordo sul livello di servizio · 56 Piano di uscita · 57 Deposito del codice (escrow)

IN ESSERE OGGI

Sicurezza, dati e IA

- **Modelli e embeddings solo nell'UE**, su Amazon Bedrock nella regione di Francoforte (UE); nessun addestramento sui dati dei clienti.
- **MFA obbligatoria** per ogni utente e su ogni console amministrativa; credenziali amministrative solo temporanee.
- **Log e rilevazione**: accessi HTTP e applicativi 90 giorni, CloudTrail con convalida d'integrità 12 mesi, GuardDuty, sonda esterna ogni minuto e allarmi 24/7.
- **Rilasci controllati**: verifica obbligatoria, branch protetti, scansione dei segreti su tutta la storia del codice.
- **Marcatura art. 50 AI Act** nei file generati e avvisi di IA nelle chat e nelle mail automatiche.

IN ESSERE OGGI

Continuità, processi, persone

- **Copie giornaliere** in Germania e in Irlanda, cifrate, conservate 14 giorni; RPO 24 ore, RTO 8 ore.
- **Prove di ripristino** automatiche a ogni verifica del codice e trimestrali sullo snapshot reale, con verbale e RTO misurato.
- **Piano di continuità** adottato; procedura degli incidenti su tre livelli; registro delle violazioni.
- **Fornitori** valutati prima dell'ingaggio e ogni anno, con DPA firmati; elenco pubblico dei subfornitori.
- **Persone**: formazione annuale su sicurezza, privacy e IA; revisione trimestrale degli accessi privilegiati; DPO esterno nominato.

Il quadro completo dei controlli in essere è nel documento 00 (Trust Center) e, controllo per controllo, nel documento 05 (Sicurezza delle informazioni).

Valore contrattuale. Per i clienti che firmano l'Allegato DORA (documento 18), l'Accordo sul livello di servizio (55) o il term sheet del deposito del codice (57), le tappe di questo documento sono impegni: «Trailgun realizza le tappe del Percorso di certificazione e piattaforma (Documento 12, versione 2.0) alle date ivi indicate». I valori che una tappa introduce, per esempio i nuovi livelli di servizio della R14, si applicano dalla data della tappa senza bisogno di modificare il contratto.

17
tappe, dal 15/12/2026 al 30/06/2028

4
verso la certificazione ISO/IEC 27001:2022

5
su continuità, copie e ripristino regionale

1
obiettivo, non impegno: la valutazione ISO/IEC 42001

CALENDARIO

Diciotto mesi, sei aree

Ogni casella è una tappa con il suo codice e la sua data. Le date sono quelle degli impegni contrattuali; un trimestre si legge per data di scadenza.

AREA	DICEMBRE 2026	T1 2027	T2 2027	T3 2027	T4 2027	2028
Continuità e copie RPO, ripristino regionale, copie immutabili	R01 · 15/12 RPO 4 ore R03 · 31/12 Ripristino in Irlanda provato	R10 · 31/03 Prova DR regionale completa R11 · 31/03 Copie protette 7 giorni				
Uscita e deposito del codice esportazione, escrow	R02 · 15/12 Esportazione in autonomia	R09 · 31/03 Codice in escrow				
Servizio e rapporti livelli di servizio, informazione		R04 · 01/01 Rapporti mensili e trimestrali		R14 · 01/07 99,9 %, RPO 15 min, RTO 4 ore		
Verifiche di sicurezza scansioni, penetration test		R05 · 01/01 Scansione esterna mensile R06 · 29/01 Primo penetration test				
Certificazione ISO/IEC 27001, ISO/IEC 42001		R07 · 29/01 Gap assessment R08 · 31/03 SGSI operativo		R15 · 30/09 Audit di stage 1	R16 · 17/12 Certificato ISO/IEC 27001	R17 · 30/06/2028 Valutazione ISO/IEC 42001 (obiettivo)
Piattaforma e organizzazione più zone, persone			R12 · 30/06 Nuova piattaforma su più zone R13 · 30/06 Responsabile della sicurezza dedicato			

impegno con data obiettivo, non impegno

I numeri che cambiano

IMPEGNO	IN ESSERE	TAPPA INTERMEDIA	DOPO LA NUOVA PIATTAFORMA (R14, 01/07/2027)
Disponibilità 24 ore su 24	99,5 % mensile	–	99,9 % mensile
Disponibilità in orario lavorativo giorni lavorativi 08:00-20:00	99,8 % mensile	–	99,95 % mensile
RPO, perdita massima di dati	24 ore	4 ore dal 15/12/2026 (R01)	15 minuti
RTO, guasto di istanza, disco o zona	8 ore	–	4 ore
RTO, perdita della regione di Francoforte	ripristino in Irlanda dalle copie	24 ore dal 01/01/2027 (R03)	12 ore
Crediti di servizio	prima fascia da 99,0 % a meno di 99,5 %	–	soglie +0,4 punti: prima fascia da 99,5 % a meno di 99,9 %

LE DICIASSETTE TAPPE

Che cosa cambia, che cosa ricevete, come lo sapete

In ordine di data. Ogni tappa completata si comunica per email agli amministratori e ai referenti sicurezza indicati nel Modulo d'ordine e, dal 01/01/2027, nel rapporto trimestrale (R04). L'evidenza si consegna su richiesta, sotto riservatezza dove indicato; ai clienti DORA con funzioni essenziali o importanti sempre.

R01 RPO 4 ore: snapshot ogni 4 ore conservati 7 giorni

15/12/2026

CHE COSA CAMBIA

Oltre alla copia giornaliera delle 02:00 UTC e a quella prima di ogni rilascio, il disco dati si copia ogni 4 ore. La perdita massima di dati in un ripristino passa da 24 a 4 ore.

EVIDENZA

Configurazione della politica delle copie ed elenco delle copie degli ultimi 7 giorni; l'RPO di 4 ore entra nell'Accordo sul livello di servizio (55).

COME LO SAPETE

Email di completamento; dal 01/01/2027 nel rapporto trimestrale con le prove di ripristino.

R02 Esportazione complessiva in autonomia

15/12/2026

CHE COSA CAMBIA

L'amministratore dello studio scarica da sé l'esportazione completa: ZIP cifrato con originali, elaborati DOCX e PDF/A, testi, dati in JSON e CSV, registri in CSV e indice con impronte SHA-256, via link temporaneo o API. Oggi la stessa esportazione si ottiene come estrazione assistita, negli stessi 10 giorni lavorativi.

EVIDENZA

Nota di rilascio della funzione; su richiesta, un'esportazione di prova su una pratica senza dati reali, con l'indice delle impronte.

COME LO SAPETE

Email di completamento e aggiornamento del Piano di uscita (56) e della procedura 28.

R03 Ripristino regionale in Irlanda: procedura scritta e provata, poi RTO regionale 24 ore

31/12/2026 · RTO dal 01/01/2027

CHE COSA CAMBIA

Se la regione di Francoforte non è disponibile, la piattaforma si ricostruisce in Irlanda (eu-west-1) dalle copie che già vi si trovano, con immagini, segreti e accessi preparati. Dal 01/01/2027 vale l'RTO regionale di 24 ore.

EVIDENZA

Procedura aggiornata nei documenti 30 (Backup e ripristino) e 31 (Prova di disaster recovery); verbale della prova con gli orari.

COME LO SAPETE

Email con la sintesi della prova; esito sempre ai clienti DORA.

R04 Rapporto di servizio mensile in app e trimestrale per email

01/01/2027

CHE COSA CAMBIA

Ogni mese l'amministratore trova in app disponibilità, incidenti, ticket e tempi; ogni trimestre riceve per email anche i cambi di subfornitori e le prove di ripristino. Trimestrale su richiesta, sempre per i clienti DORA con funzioni essenziali o importanti.

EVIDENZA

Il rapporto stesso, con la disponibilità misurata dalla sonda esterna minuto per minuto.

COME LO SAPETE

Il primo rapporto mensile in app a febbraio 2027 per gennaio; il primo trimestrale ad aprile 2027.

R05 Scansione esterna mensile dell'applicazione

01/01/2027

CHE COSA CAMBIA

Alle scansioni già attive (ogni immagine in ECR, dipendenze ogni settimana, segreti a ogni verifica) si aggiunge ogni mese una scansione dall'esterno dell'applicazione esposta. Le correzioni seguono i tempi in essere: critica 72 ore, alta 7 giorni, media 30, bassa 90.

EVIDENZA

Sintesi mensile con numero di rilievi per gravità e stato di correzione.

COME LO SAPETE

Nel rapporto trimestrale (R04).

R06 Primo penetration test indipendente, poi ogni anno e dopo ogni cambiamento rilevante

29/01/2027

CHE COSA CAMBIA

Un terzo indipendente prova l'applicazione, le API e l'infrastruttura. Il test si ripete ogni anno e dopo ogni cambiamento rilevante dell'architettura, a partire dalla nuova piattaforma (R12). Trailgun partecipa inoltre ai test guidati dalla minaccia (TLPT) del Cliente, alle condizioni concordate.

EVIDENZA

Sintesi esecutiva del rapporto e piano di rimedio con le date, sotto riservatezza; conferma della chiusura dei rilievi critici e alti.

COME LO SAPETE

Email con la sintesi appena ricevuto il rapporto finale del tester.

R07 Gap assessment ISO/IEC 27001:2022

29/01/2027

CHE COSA CAMBIA

Un consulente esterno confronta il sistema di gestione e i 93 controlli dell'Allegato A con la norma e fissa il piano verso la certificazione. Il punto di partenza è la dichiarazione di applicabilità del documento 14.

EVIDENZA

Sintesi del gap assessment con le azioni e le date.

COME LO SAPETE

Email e aggiornamento del documento 14.

R08 SGSI operativo: politiche, rischi, dichiarazione di applicabilità definitiva

31/03/2027

CHE COSA CAMBIA

Il sistema di gestione della sicurezza delle informazioni gira con i suoi cicli: riesame della direzione, audit interno, registro dei rischi (41) aggiornato, obiettivi misurati. È la condizione per l'audit di certificazione.

EVIDENZA

Dichiarazione di applicabilità definitiva (14), verbale del riesame della direzione, sintesi dell'audit interno.

COME LO SAPETE

Email e nuova versione dei documenti 14 e 41.

R09 Deposito del codice presso un agente di escrow, aggiornato ogni trimestre

31/03/2027

CHE COSA CAMBIA

Codice sorgente, infrastruttura come codice e istruzioni di ricostruzione si depositano presso un agente terzo, [AGENTE DI ESCROW], e si aggiornano ogni trimestre. Rilascio al beneficiario per insolvenza, cessazione dell'attività o del Servizio senza subentro. Fino ad allora vale l'esportazione garantita dei dati.

EVIDENZA

Lettera dell'agente con la data dell'ultimo deposito e la verifica di integrità; adesione del Cliente beneficiario come da term sheet (57).

COME LO SAPETE

Email ai clienti che hanno chiesto l'adesione; conferma a ogni deposito trimestrale.

R10 Prima prova completa di ripristino regionale, poi ogni anno

31/03/2027

CHE COSA CAMBIA

Si simula la perdita della regione di Francoforte e si ricostruisce l'intero servizio in Irlanda, misurando l'RTO regionale contro l'impegno di 24 ore. La prova si ripete ogni anno, accanto alle prove trimestrali in essere.

EVIDENZA

Verbale della prova DR secondo il programma del documento 31: scenario, orari, RTO e RPO misurati, scostamenti e azioni.

COME LO SAPETE

Email con la sintesi; esito sempre ai clienti DORA.

R11 Copie protette dalla cancellazione per 7 giorni

31/03/2027

CHE COSA CAMBIA

Le copie di sicurezza diventano immutabili per 7 giorni con EBS Snapshot Lock o AWS Backup Vault Lock: nemmeno un amministratore con credenziali valide, o chi le avesse sottratte, può cancellarle prima.

EVIDENZA

Configurazione del blocco mostrata in audit; voce aggiornata nei documenti 05, 30 e P09.

COME LO SAPETE

Email di completamento e rapporto trimestrale.

R12 Nuova piattaforma su più zone di disponibilità

30/06/2027

CHE COSA CAMBIA

Container senza stato su ECS Fargate dietro un Application Load Balancer con WAF; database gestito Aurora PostgreSQL con ripristino a un istante; file su S3 con versioning e chiavi KMS di Trailgun; AWS Backup con copie in Irlanda e blocco; lavorazioni in una coda che sopravvive ai rilasci, che quindi non interrompono più il lavoro in corso.

EVIDENZA

Descrizione dell'architettura aggiornata (05); preavviso di manutenzione per la migrazione secondo l'Accordo sul livello di servizio; penetration test dopo il cambiamento (R06).

COME LO SAPETE

Comunicazione della finestra di migrazione con almeno 48 ore di preavviso, come ogni manutenzione programmata, ed email a migrazione conclusa.

R13 Responsabile della sicurezza dedicato

30/06/2027

CHE COSA CAMBIA

La funzione di responsabile della sicurezza passa a una persona dedicata. Fino ad allora la ricopre ad interim il CEO, Franco Puppo, con le compensazioni del documento 05: infrastruttura come codice, rilasci automatizzati e protetti, accesso di emergenza documentato.

EVIDENZA

Nome, ruolo e contatti della persona nominata; organigramma della sicurezza aggiornato.

COME LO SAPETE

Email ai referenti sicurezza; aggiornamento di 00, 05 e P01.

R14 Nuovi livelli di servizio

01/07/2027

CHE COSA CAMBIA

Disponibilità 99,9 % mensile (99,95 % nei giorni lavorativi 08:00-20:00); RPO 15 minuti; RTO 4 ore, 12 ore per la perdita della regione. Le soglie dei crediti di servizio salgono di 0,4 punti: la prima fascia va da 99,5 % a meno di 99,9 %.

EVIDENZA

Accordo sul livello di servizio (55), dove i nuovi valori sono già scritti con la loro data; disponibilità misurata nel rapporto mensile.

COME LO SAPETE

Email di entrata in vigore; i valori valgono senza modifiche contrattuali.

R15 Audit di stage 1 ISO/IEC 27001

30/09/2027

CHE COSA CAMBIA

L'organismo di certificazione accreditato, [ENTE DI CERTIFICAZIONE], verifica la documentazione e la prontezza del sistema di gestione per l'audit di stage 2.

EVIDENZA

Esito dello stage 1 con le eventuali aree di attenzione e il piano per chiuderle.

COME LO SAPETE

Email con la sintesi.

R16 Certificato ISO/IEC 27001:2022

17/12/2027

CHE COSA CAMBIA

Trailgun è certificata ISO/IEC 27001:2022 con ambito «piattaforma Trailgun e processi di supporto». Il certificato si mantiene con audit di sorveglianza annuali e si rinnova ogni tre anni.

EVIDENZA

Certificato con ambito e dichiarazione di applicabilità della versione certificata.

COME LO SAPETE

Email e pubblicazione sul sito; aggiornamento di 00, 05, 13 e 14.

R17 Valutazione ISO/IEC 42001 (obiettivo, non impegno)

30/06/2028

CHE COSA CAMBIA

Trailgun valuta il sistema di gestione dell'intelligenza artificiale rispetto alla ISO/IEC 42001:2023, partendo dalla politica di governance dell'IA (P15) e dal documento 09. È un obiettivo dichiarato, non un impegno contrattuale.

EVIDENZA

Esito della valutazione e decisione sulla certificazione.

COME LO SAPETE

Email e aggiornamento dei documenti 09 e P15.

CERTIFICAZIONI

Che cosa vale prima del certificato

Trailgun non dichiara certificazioni proprie prima della tappa R16. Per l'infrastruttura valgono quelle di AWS.

STANDARD O VERIFICA	STATO AL 01/12/2026	CHE COSA TROVATE NEL PACCHETTO
ISO/IEC 27001:2022	Percorso R07, R08, R15, R16; certificato il 17/12/2027	Dichiarazione di applicabilità dei 93 controlli dell'Allegato A, con stato ed evidenza (14); 17 politiche (P01-P17) e 12 procedure (20-31)
Infrastruttura AWS	Ereditate: ISO/IEC 27001, 27017, 27018, SOC 2, C5	Rapporti da AWS Artifact su richiesta
Penetration test	Primo il 29/01/2027 (R06), poi ogni anno	Sintesi e piano di rimedio, sotto riservatezza
Scansioni di vulnerabilità	Immagini, dipendenze e segreti in essere; scansione esterna mensile dal 01/01/2027 (R05)	Tempi di correzione nel documento 24 e nella politica P07
ISO/IEC 42001	Valutazione entro il 30/06/2028 (R17), come obiettivo	Documento 09 e politica P15
SOC 2, ISO 22301, ISO/IEC 27701	Non pianificate	Le risposte equivalenti sono nel questionario precompilato (13); la continuità è nel documento 11

Fino al certificato il Cliente ha a disposizione gli elementi di garanzia che il Regolamento delegato (UE) 2024/1773, art. 6, par. 3, ammette per valutare un fornitore: i propri audit, ai sensi del contratto (uno all'anno; illimitati per le funzioni essenziali o importanti DORA e per le autorità); i rapporti indipendenti, come il penetration test; gli audit interni di Trailgun; le informazioni del fornitore, cioè questo Pacchetto, con le evidenze indicate nella dichiarazione di applicabilità (14) e nei registri 40-45, che si mostrano in sede di audit. L'art. 8, par. 3, lett. f), dello stesso Regolamento chiede che una certificazione comprenda la prova dell'efficacia operativa dei controlli: per questo il percorso arriva al certificato dopo un ciclo completo del sistema di gestione.

INFORMAZIONE E GOVERNO DEL PERCORSO

Come vi teniamo informati

QUANDO	CHE COSA RICEVETE
A ogni tappa completata	Email agli amministratori e ai referenti sicurezza del Modulo d'ordine, con l'evidenza disponibile o il modo di chiederla
Ogni mese, dal 01/01/2027	Rapporto di servizio in app: disponibilità, incidenti, ticket e tempi
Ogni trimestre, dal 01/01/2027	Rapporto per email con lo stato del Percorso, i cambi di subfornitori e le prove di ripristino
Se una data si sposta	Email con la nuova data, il motivo e le misure che compensano il ritardo, appena il ritardo è prevedibile e comunque prima della data; ai clienti DORA con le conseguenze contrattuali dell'Allegato DORA (18)
Su richiesta	Stato aggiornato del Percorso entro 15 giorni lavorativi, nell'ambito dei questionari del cliente; contatto security@trailgun.ai

Il Percorso si riesamina a ogni tappa completata e almeno ogni trimestre nel riesame della sicurezza; le date si cambiano solo con una nuova versione di questo documento, approvata dall'organo amministrativo e comunicata ai clienti. Titolare del Percorso è il responsabile della sicurezza.

SUMMARY IN ENGLISH

Certification and platform roadmap

This is the only document of the Trailgun compliance pack that contains future dates. Everything else in the pack describes the platform as it is on 1 December 2026. For clients who sign the DORA annex (document 18), the SLA (55) or the escrow term sheet (57), the milestones below are binding by reference.

CODE	DATE	MILESTONE
R01	15 Dec 2026	RPO 4 hours: snapshots every 4 hours, kept 7 days
R02	15 Dec 2026	Self-service full export (encrypted ZIP, JSON/CSV, SHA-256 index); until then assisted export within the same 10 business days
R03	31 Dec 2026	Regional recovery in Ireland written and tested; regional RTO 24 hours from 1 Jan 2027
R04	1 Jan 2027	Monthly service report in the app, quarterly report by email
R05	1 Jan 2027	Monthly external application scan
R06	29 Jan 2027	First independent penetration test, then yearly and after major changes; summary and remediation plan to clients
R07	29 Jan 2027	ISO/IEC 27001:2022 gap assessment
R08	31 Mar 2027	ISMS operational: policies, risk register, final Statement of Applicability
R09	31 Mar 2027	Source code escrow with a third-party agent, updated quarterly
R10	31 Mar 2027	First full regional disaster recovery test, then yearly
R11	31 Mar 2027	Backups protected from deletion for 7 days (Snapshot Lock or Backup Vault Lock)
R12	30 Jun 2027	Multi-AZ platform: ECS Fargate behind ALB with WAF, Aurora PostgreSQL with PITR, S3 with versioning and Trailgun KMS keys, AWS Backup with copies in Ireland and lock, a queue that survives releases
R13	30 Jun 2027	Dedicated security officer
R14	1 Jul 2027	New service levels: 99.9 % (99.95 % in business hours), RPO 15 minutes, RTO 4 hours (12 hours regional), credit thresholds +0.4 points
R15	30 Sep 2027	ISO/IEC 27001 stage 1 audit
R16	17 Dec 2027	ISO/IEC 27001:2022 certificate (Trailgun platform and supporting processes)
R17	30 Jun 2028	ISO/IEC 42001 assessment (objective, not a commitment)

Until the certificate, AWS certifications apply to the infrastructure (ISO/IEC 27001, 27017, 27018, SOC 2, C5; reports from AWS Artifact on request), and clients rely on their own audits, independent reports, Trailgun's internal audits and this pack (Delegated Regulation (EU) 2024/1773, art. 6(3)). Each completed milestone is notified by email and, from 1 January 2027, in the quarterly report. Contact: security@trailgun.ai.