Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO 08

VERSIONE 2.0 · DICEMBRE 2026

DORA: Trailgun come fornitore ICT

Come Trailgun copre gli artt. 28, 29 e 30 del Regolamento (UE) 2022/2554 e i suoi atti di livello 2: classificazione del servizio, clausole, registro delle informazioni, catena di subfornitura, concentrazione, incidenti, test, audit, uscita e continuità. Con l'Allegato DORA da firmare, la Mappa DORA, la Scheda per il Registro delle informazioni, l'SLA, il piano di uscita e i modelli di notifica.

SOGGETTO OBBLIGATO	TRAILGUN	TIPO DI SERVIZIO	DATI E MODELLI
Il Cliente, entità finanziaria	Fornitore terzo di servizi TIC	S19 · Cloud SaaS	AWS, regioni UE

INDICE

Una sezione per ogni domanda dell'ufficio fornitori

Ogni affermazione sulla piattaforma descrive lo stato al 01/12/2026, con un'evidenza mostrabile in audit. Le tappe successive hanno un codice (R01-R17) e una data nel documento 12, Percorso di certificazione e piattaforma. I numeri degli impegni sono gli stessi in tutti i documenti del pacchetto di conformità.

01 Chi è soggetto a DORA, e perché Trailgun semplifica il lavoro
Il Cliente è obbligato; Trailgun è fornitore terzo di servizi TIC, non fornitore critico

02 Funzione essenziale o importante: come classificare Trailgun
Uso per uso, gli elementi per la valutazione del Cliente

03 Art. 28 e art. 29, punto per punto
Principi, registro, due diligence, risoluzione, uscita, concentrazione, subappalto

04 Art. 30, par. 1 e 2: le clausole per ogni contratto

05 Art. 30, par. 3: le clausole per le funzioni essenziali o importanti

06 La politica e la gestione del rischio del Cliente
Reg. del. (UE) 2024/1773 e 2024/1774, mappati

07 Registro delle informazioni
I campi del Reg. es. (UE) 2024/2956 che riguardano Trailgun e il contratto

08 Catena di subfornitura e Reg. del. (UE) 2025/532

09 Rischio di concentrazione: AWS

10 Incidenti: i tempi di Trailgun dentro quelli del Cliente

11 Test di resilienza e TLPT

12 Accesso, ispezione e audit, anche della Banca d'Italia

13 Strategia di uscita e piano di transizione

14 Continuità operativa e livelli di servizio

15 Che cosa è in essere, e il Percorso

16 Contatti, documenti collegati e riferimenti normativi

EN English summary

COME LEGGERE IL DOCUMENTO

Gli stati, scritti sempre

Nelle tabelle ogni presidio porta uno di questi stati. Gli impegni contrattuali sono ripresi nell'Allegato DORA (documento 18) e nell'Accordo sul livello di servizio (documento 55).

IN ESSERE
Il presidio esiste sulla piattaforma o nell'organizzazione, con un'evidenza che il Cliente può verificare in audit.

ALLA FIRMA
Obbligo contrattuale di Trailgun che vale dalla sottoscrizione dell'Allegato DORA.

PERCORSO R01-R17
Tappa successiva, con data ed evidenza attesa nel documento 12; vincolante per rinvio dell'Allegato DORA.

IN BREVE

- DORA obbliga il Cliente, cioè l'entità finanziaria. Trailgun è un «fornitore terzo di servizi TIC» (art. 3, punto 19) e presta un «servizio TIC» (art. 3, punto 21) di tipo S19, Cloud SaaS.
- Per gli intermediari ex art. 106 TUB gli artt. 28, 29 e 30 si applicano dal 1° gennaio 2027 (artt. 6 e 17 del D.Lgs. 23/2025). L'Allegato DORA è pronto da firmare.
- Trailgun non è un fornitore critico designato (artt. 31 ss.). La vigilanza su Trailgun passa dal contratto con il Cliente e dai poteri di accesso e ispezione delle autorità italiane (art. 8 D.Lgs. 23/2025).
- Ogni lettera dell'art. 30, par. 2 e 3, ha un articolo dell'Allegato DORA, firmabile così com'è. Ogni campo del registro delle informazioni che riguarda Trailgun ha un valore nella Scheda (documento 16).
- Trailgun notifica un incidente TIC entro 2 ore da quando ne viene a conoscenza. Al Cliente resta margine per la sua notifica iniziale, dovuta entro 4 ore dalla classificazione e comunque entro 24 ore dalla conoscenza.
- Infrastruttura, dati e modelli di intelligenza artificiale sono su AWS nelle regioni dell'Unione. La sezione 15 elenca i presidi in essere e le tappe del Percorso.

01 · AMBITO

Chi è soggetto a DORA, e perché Trailgun semplifica il lavoro

Il Regolamento (UE) 2022/2554 («DORA») si applica alle entità finanziarie dal 17 gennaio 2025 (art. 64). Il fornitore non ha obblighi propri di DORA, ma il Cliente può rispettare i suoi solo se il fornitore gli dà clausole, informazioni e prove.

SOGGETTO	DORA SI APPLICA?	BASE	CHE COSA SERVE DA TRAILGUN
Banca (ente creditizio)	Sì, regime ordinario	Art. 2, par. 1, lett. a); artt. 5-15 e 28-30	Tutto questo documento. TLPT se la banca è individuata dall'autorità (art. 26)
Intermediario ex art. 106 TUB (servicer, master servicer)	Sì, dal 1° gennaio 2027, regime semplificato dell'art. 16	Art. 6, c. 1, e art. 17 D.Lgs. 23/2025; consultazione della Banca d'Italia del 30 settembre 2026	Artt. 28 (salvo par. 2), 29 e 30, par. 1-4. Gli artt. 26-27 (TLPT) non si applicano
Altre entità dell'art. 2 (istituti di pagamento e di moneta elettronica, imprese di investimento, gestori di fondi, assicurazioni)	Sì, secondo il regime di ciascuna	Art. 2, par. 1, DORA; art. 16 per i soggetti del regime semplificato	Come per la banca, nei limiti del regime
Gestore di crediti in sofferenza ex art. 114.6 TUB che non è un 106	No	D.Lgs. 116/2024; disposizioni della Banca d'Italia del 13 febbraio 2025	Clausole di esternalizzazione e disponibilità alle ispezioni della Banca d'Italia (art. 114.11 TUB). Può chiedere l'applicazione dell'Allegato DORA; mappa delle linee guida EBA nel documento 48
Studio legale	No: non è un'entità finanziaria	–	Può consegnare questo documento alla banca o al servicer per cui lavora

SOGGETTO	DORA SI APPLICA?	BASE	CHE COSA SERVE DA TRAILGUN
Trailgun	Non come soggetto obbligato	Art. 8 D.Lgs. 23/2025; art. 144, c. 8-bis, TUB	Come fornitore di un servizio che sostiene funzioni essenziali o importanti è soggetta ai poteri di accesso e ispezione delle autorità e alle sanzioni per mancata collaborazione

1.1 Perché Trailgun non è un fornitore critico

I fornitori critici (CTPP) sono designati dalle autorità europee di vigilanza secondo i criteri cumulativi dell'art. 31, par. 2: impatto sistemico, carattere sistemico delle entità servite, dipendenza delle funzioni essenziali o importanti, sostituibilità. Il Reg. del. (UE) 2024/1502 fissa una prima soglia del 10 % del numero o del totale attivo di una categoria di entità servite (art. 2, par. 4). Trailgun è molto al di sotto. Finché serve solo entità finanziarie attive solo in Italia, rientra anche nell'esclusione dell'art. 31, par. 8, punto iv).

L'elenco dei fornitori critici designati il 18 novembre 2025 conta 19 fornitori, tra cui **Amazon Web Services EMEA SARL**, l'infrastruttura su cui girano Trailgun e i suoi modelli (sezione 9).

La conseguenza pratica è che su Trailgun non vigila il Lead Overseer: vigilano il Cliente, con il contratto dell'art. 30, e le autorità nazionali, con l'art. 8 del D.Lgs. 23/2025.

1.2 Trailgun e la NIS2

Un SaaS è in astratto un «servizio di cloud computing» (considerando 33 della direttiva (UE) 2022/2555), ma per questo settore vale la soglia della media impresa (art. 3 D.Lgs. 138/2024). Trailgun è sotto la soglia e fuori dall'ambito della NIS2; lo riesamina ogni anno e quando cambiano addetti o fatturato. Per le entità finanziarie DORA è comunque norma speciale (art. 4 della direttiva; art. 15 D.Lgs. 23/2025). La posizione completa, con il supporto alla sicurezza della catena di approvvigionamento dei clienti NIS2, è nel documento 62.

1.3 Sanzioni e cooperazione

L'art. 144, c. 8-bis, TUB, introdotto dall'art. 10 del D.Lgs. 23/2025, sanziona anche il fornitore terzo di servizi TIC per l'«omessa collaborazione o mancato seguito dato nell'ambito di un'indagine, un'ispezione o una richiesta» ai sensi dell'art. 8, con sanzioni da 30.000 euro fino al 10 % del fatturato. Per Trailgun cooperare con la Banca d'Italia è quindi anche un obbligo di legge, e l'Allegato DORA lo scrive come obbligo verso il Cliente (art. 10 dell'Allegato).

1.4 Che cosa consegna Trailgun

- **Questo documento**, con la copertura di ogni requisito, il suo stato e la sua evidenza.
- **Allegato DORA al contratto** (documento 18, Word, firmabile). Copre ogni lettera dell'art. 30, par. 2 e 3, gli artt. 28, par. 7 e 8, e 29 e il Reg. del. 2025/532.
- **Mappa DORA** (documento 17, Excel): requisito, clausola di Trailgun, documento e sezione, evidenza, stato.
- **Scheda per il Registro delle informazioni** (documento 16, Excel): i campi del Reg. es. (UE) 2024/2956 che riguardano Trailgun e il contratto, già compilati, e la catena di subfornitura con i ranghi.
- **Accordo sul livello di servizio** (55), **Piano di uscita e di transizione** (56), **term sheet del deposito del codice** (57), **Modelli di notifica degli incidenti** (51), **Mappa delle linee guida EBA sull'esternalizzazione** (48).
- **Gli altri documenti del pacchetto**: Contratto di servizio, Sicurezza delle informazioni (05), Protezione dei dati (06) e DPA (07), AI Act (09), Politiche (10, P01-P17), Continuità operativa (11), Percorso (12), Questionario (13). I numeri degli impegni sono gli stessi in tutti.

02 · CLASSIFICAZIONE

Funzione essenziale o importante: la valuta il Cliente

Per l'art. 3, punto 22, è essenziale o importante la funzione la cui interruzione «comprometterebbe sostanzialmente» i risultati finanziari, la solidità o la continuità dei servizi dell'entità, o il rispetto delle condizioni della sua autorizzazione. La qualifica riguarda la funzione del Cliente che il servizio sostiene. Il fornitore non può darla né escluderla in astratto.

USO DI TRAILGUN	FUNZIONE DEL CLIENTE	LETTURA DI TRAILGUN, DI REGOLA	ELEMENTI CHE SPINGONO VERSO «ESSENZIALE O IMPORTANTE»
Ricorso per decreto ingiuntivo	Recupero giudiziale dei crediti	Di regola non essenziale: l'avvocato rivede ogni atto e può redigerlo senza la piattaforma	Una quota rilevante del recupero passa da Trailgun; scadenze (prescrizione, termini processuali) gestite solo in piattaforma; nessuna procedura alternativa pronta
Insinuazione al passivo	Recupero nelle procedure concorsuali	Come sopra; il tempo conta per i termini delle domande	Domande concentrate in pochi giorni, senza alternativa operativa
Escussione delle garanzie pubbliche (Fondo PMI, SACE, ISMEA)	Attivazione delle garanzie, con i termini delle disposizioni dei garanti	Può diventarlo: un ritardo incide direttamente sui risultati finanziari	Volumi alti, termini vicini, nessuna procedura manuale dimensionata
Remediation del data tape	Qualità dei dati dei portafogli e delle cartolarizzazioni	Più probabile: il data tape alimenta obblighi informativi verso investitori e vigilanza	Il data tape corretto va in segnalazione o nei report senza altri controlli del Cliente
Assessment (due diligence R&W)	Valutazione di portafogli ceduti o acquistati	Di regola no: lavoro a progetto, non continuativo	Uso per decisioni di acquisto con scadenze vincolanti
Analisi del faldone, trattative, ricerca fonti	Supporto al contenzioso e alla contrattualistica	Di regola no	–

2.1 Le domande da farsi

1. **Interruzione.** Che cosa succede se Trailgun resta ferma per 5 giorni lavorativi, il periodo massimo tollerabile di interruzione assunto da Trailgun? Il Cliente ha una procedura manuale? Gli elaborati già scaricati bastano per depositare?
2. **Quota.** Quante pratiche, o quale parte del portafoglio, passano dalla piattaforma?
3. **Scadenze.** L'uso è legato a termini di legge o contrattuali che non si possono spostare?
4. **Obblighi regolamentari.** Il risultato alimenta segnalazioni di vigilanza o obblighi informativi delle cartolarizzazioni?
5. **Dati.** Dati giudiziari, anche penali, dati coperti da segreto bancario o professionale: la sensibilità è alta (campo B_02.02.0170 del registro).
6. **Sostituibilità.** Esportare i dati e passare ad altro fornitore, o tornare al lavoro manuale, quanto costa e quanto dura (sezione 13)?

La colonna «Lettura di Trailgun» non è una valutazione. Serve al Cliente per motivare la propria nel modello B_06.01 del registro, campi 0050 e 0060.

2.2 Che cosa cambia se la funzione è essenziale o importante

- Si applicano anche le clausole dell'art. 30, par. 3: la Sezione B dell'Allegato DORA. Per attivarla basta la dichiarazione del Cliente nell'Allegato (art. 3), senza nuova trattativa.
- Il Cliente deve avere una strategia di uscita documentata e testata (art. 28, par. 8): Trailgun gli fornisce il piano di transizione della sezione 13 e del documento 56.
- Il Cliente valuta la concentrazione e il subappalto (art. 29): sezioni 8 e 9.
- Il preavviso sui cambi rilevanti dei subfornitori sale da 30 a 60 giorni (Reg. del. 2025/532).
- I diritti di accesso, ispezione e audit diventano illimitati (sezione 12).
- Nel registro entra la catena di subfornitura (B_05.02) e il Cliente informa tempestivamente l'autorità dell'accordo previsto (art. 28, par. 3).
- Se la classificazione cambia durante il contratto, il Cliente lo comunica e la Sezione B si applica dalla comunicazione.

03 · ARTT. 28 E 29

Art. 28: principi generali, registro, uscita

Ai 106 si applicano tutti i paragrafi salvo il 2 (art. 6 D.Lgs. 23/2025). Le clausole citate sono gli articoli dell'Allegato DORA.

ART. 28	CHE COSA CHIEDE AL CLIENTE	CHE COSA FORNISCE TRAILGUN	DOVE	STATO
Par. 1, a)	Resta pienamente responsabile anche quando usa servizi di terzi	Nessuna clausola limita gli obblighi del Cliente verso le autorità; trasparenza completa con questo documento e la Mappa	All. art. 2	IN ESSERE
Par. 1, b)	Proporzionalità	Gli elementi per dimensionare: tipo di servizio, dati, sostituibilità, catena	Sez. 2, 7, 8	IN ESSERE
Par. 2	Strategia e politica sui fornitori (non per i 106, l'art. 16 e le microimprese)	Mappatura del Reg. del. 2024/1773 requisito per requisito	Sez. 6	IN ESSERE
Par. 3	Registro delle informazioni; segnalazione almeno annuale; informativa tempestiva sugli accordi per funzioni essenziali o importanti	Scheda per il Registro già compilata (documento 16), con il LEI di Trailgun [LEI], aggiornata da Trailgun a ogni cambiamento	Sez. 7; All. art. 22	IN ESSERE
Par. 4	Valutazione prima del contratto: funzione, rischi, concentrazione, due diligence, conflitti di interesse	Questionario precompilato (documento 13); risposta ai questionari del Cliente entro 15 giorni lavorativi, una volta l'anno senza costi; dichiarazione dei conflitti di interesse su richiesta; dati societari nella Scheda	Sez. 2, 9, 12	IN ESSERE
Par. 5	Fornitori con norme adeguate di sicurezza; per le funzioni essenziali o importanti, le più aggiornate	Politiche P01-P17 e dichiarazione di applicabilità rispetto a ISO/IEC 27001:2022 (documenti 10 e 14); infrastruttura certificata da AWS (ISO 27001, 27017, 27018, SOC 2, C5). Certificazione di Trailgun: tappe R07, R08, R15, R16 del Percorso	Sez. 15; doc. 12	IN ESSERE PERCORSO R16
Par. 6	Diritti di accesso, ispezione e audit secondo il rischio	Audit ordinario 1 volta l'anno con 30 giorni di preavviso; illimitati per le funzioni essenziali o importanti e per le autorità	Sez. 12; All. art. 17	ALLA FIRMA
Par. 7, a)-d)	Cause di risoluzione	Tutte e quattro sono cause di risoluzione del Contratto da parte del Cliente	All. art. 11	ALLA FIRMA
Par. 8	Strategie di uscita per le funzioni essenziali o importanti	Piano di uscita e di transizione (documento 56), assistenza fino a 12 mesi, esportazione completa, cancellazione certificata; deposito del codice presso un terzo (documento 57)	Sez. 13; All. artt. 18 e 21	ALLA FIRMA ESCROW: PERCORSO R09

Art. 29: concentrazione e subappalto

Si applica solo ai servizi che sostengono funzioni essenziali o importanti.

ART. 29	ELEMENTO DELLA VALUTAZIONE DEL CLIENTE	INFORMAZIONE DI TRAILGUN
Par. 1	Fornitore «non facilmente sostituibile»; più accordi con lo stesso fornitore o con fornitori connessi	Un contratto per Cliente, per tutti i verticali. Fornitore sottostante: AWS, per infrastruttura e modelli, che probabilmente è già nel registro del Cliente (sezione 9)
Par. 2, benefici e rischi del subappalto	In particolare per i subappaltatori stabiliti in paesi terzi	Catena completa nella sezione 8, con sede, luogo dei dati e rango di ciascuno
Par. 2, diritto fallimentare	Diritto fallimentare del fornitore e vincoli al recupero urgente dei dati	Trailgun è una società a responsabilità limitata di diritto italiano: si applica il Codice della crisi d'impresa e dell'insolvenza (D.Lgs. 14/2019). Per il recupero urgente: esportazione dalla piattaforma in ogni momento e deposito del codice presso un terzo (sezione 13)
Par. 2, paesi terzi	Protezione dei dati e applicazione effettiva della legge	Dati, copie e modelli nell'Unione (Germania, Irlanda, regioni UE di Bedrock). I subfornitori con sede o capogruppo negli Stati Uniti sono indicati uno per uno (sezione 8), con la base dei trasferimenti

ART. 29	ELEMENTO DELLA VALUTAZIONE DEL CLIENTE	INFORMAZIONE DI TRAILGUN
Par. 2, catene lunghe	Effetto sul monitoraggio e sulla vigilanza	Catena di al massimo tre ranghi, dichiarata per intero

04 · ART. 30, PAR. 1 E 2

Le clausole per ogni contratto di servizi TIC

Valgono per ogni Cliente soggetto a DORA, anche se la funzione non è essenziale o importante: Sezione A dell'Allegato DORA.

ART. 30	REQUISITO	ALLEGATO	IMPEGNO DI TRAILGUN	STATO
Par. 1	Diritti e obblighi per iscritto, SLA compresi, in un unico documento durevole e accessibile	Art. 2	Modulo d'ordine, Condizioni generali, Accordo sul livello di servizio, DPA e Allegato DORA formano un unico documento, consegnato al Cliente in PDF firmato e scaricabile	ALLA FIRMA
a)	Descrizione di funzioni e servizi; se il subappalto è ammesso e a quali condizioni	Art. 4	Servizi descritti nel Contratto e nell'SLA. Subappalto ammesso solo verso i subfornitori dell'elenco, alle condizioni dell'art. 19 dell'Allegato	ALLA FIRMA
b)	Luoghi del servizio e dei dati, compresa la conservazione; preavviso dei cambiamenti	Art. 5	Dati a riposo in Germania (AWS eu-central-1); copie di sicurezza in Irlanda (eu-west-1); modelli ed embeddings su Amazon Bedrock nelle regioni UE, con le regioni fuori dall'Unione rifiutate dal codice. Preavviso di 30 giorni, 60 per le funzioni essenziali o importanti	IN ESSERE
c)	Disponibilità, autenticità, integrità e riservatezza dei dati, anche personali	Art. 6	DPA e misure del documento 05: cifratura AES-256 a riposo, TLS in transito, autenticazione a due fattori per tutti, isolamento per studio, versioni dell'atto con autore e motivo, impronte SHA-256 del pacchetto di deposito	IN ESSERE
d)	Accesso, recupero e restituzione dei dati in formato facilmente accessibile, anche per insolvenza o cessazione del fornitore	Art. 7	30 giorni di accesso in sola lettura con esportazione dopo la cessazione; esportazione complessiva in formati aperti entro 10 giorni lavorativi dalla richiesta, con certificato di restituzione; deposito del codice presso un terzo (documento 57)	ALLA FIRMA ESPORTAZIONE IN AUTONOMIA R02; ESCROW R09
e)	Livelli di servizio, con aggiornamenti e revisioni	Art. 8	Disponibilità 99,5 % mensile 24/7 e 99,8 % nei giorni lavorativi 08:00-20:00; tempi dell'assistenza per priorità (sezione 14; documento 55). Livelli successivi alla nuova piattaforma: Percorso R14	ALLA FIRMA
f)	Assistenza negli incidenti TIC, senza costi aggiuntivi o a costo determinato ex ante	Art. 9	Assistenza senza costi aggiuntivi; notifica iniziale entro 2 ore, aggiornamenti almeno ogni 24 ore, relazione intermedia entro 48 ore, finale entro 20 giorni (modelli del documento 51)	ALLA FIRMA
g)	Cooperazione piena con le autorità competenti e di risoluzione e con le persone da esse nominate	Art. 10	Cooperazione piena, compresi accessi, ispezioni e convocazioni ai sensi dell'art. 8 D.Lgs. 23/2025	ALLA FIRMA
h)	Diritti di risoluzione e periodi minimi di preavviso	Art. 11	Risoluzione nei casi dell'art. 28, par. 7, con il preavviso richiesto dall'autorità del Cliente; recesso ordinario con 90 giorni di preavviso (art. 20 CG); Trailgun recede solo se cessa il Servizio per tutti i clienti, e anche allora garantisce il periodo di transizione	ALLA FIRMA
i)	Partecipazione ai programmi di sensibilizzazione e formazione del Cliente (art. 13, par. 6)	Art. 12	Partecipazione su richiesta, a condizioni concordate. Formazione interna su sicurezza, privacy e IA all'ingresso e ogni anno, registrata (documento 43)	IN ESSERE

05 · ART. 30, PAR. 3

Le clausole per le funzioni essenziali o importanti

Sezione B dell'Allegato DORA. Si attiva con la dichiarazione del Cliente e si aggiunge alla Sezione A.

ART. 30.3	REQUISITO	ALLEGATO	IMPEGNO DI TRAILGUN	STATO
a)	Livelli di servizio con obiettivi quantitativi e qualitativi precisi; azioni correttive senza indebito ritardo	Art. 13	Obiettivi: disponibilità misurata ogni minuto da una sonda esterna, tempi di presa in carico e di soluzione per priorità, RPO, RTO, tempi di notifica. Se un obiettivo è mancato: crediti di servizio e piano di rimedio scritto, senza indebito ritardo	ALLA FIRMA
b)	Preavvisi e obblighi di segnalazione, compresi gli sviluppi che possono incidere sulla capacità di prestare il servizio	Art. 14	Avviso senza ritardo degli sviluppi rilevanti; minacce significative entro 24 ore; su richiesta, disponibilità del mese, esiti delle prove di ripristino, cambi di subfornitori. Rapporto di servizio mensile in app e trimestrale per email: Percorso R04	ALLA FIRMA RAPPORTI: PERCORSO R04
c)	Piani di emergenza attuati e testati; misure, strumenti e politiche di sicurezza adeguati	Art. 15	Piano di continuità operativa e di ripristino adottato (documento 11), rivisto e provato ogni anno. Prova di ripristino trimestrale sullo snapshot reale, con verbale; prova automatica a ogni rilascio. Prova di ripristino regionale annuale: Percorso R10	IN ESSERE
d)	Partecipazione e cooperazione piena al TLPT (artt. 26-27)	Art. 16	Partecipazione ai test guidati dalla minaccia del Cliente, anche in forma congiunta (art. 26, par. 4), alle condizioni concordate per non mettere a rischio gli altri clienti	ALLA FIRMA
e) i)	Diritti illimitati di accesso, ispezione e audit del Cliente, di un terzo nominato e dell'autorità, con copie in loco, non limitati da altri accordi	Art. 17.1	Riconosciuti senza limiti di numero; nessun altro contratto di Trailgun li può limitare	ALLA FIRMA
e) ii)	Livelli alternativi di garanzia se sono toccati i diritti di altri clienti	Art. 17.3	Audit congiunti con altri clienti, rapporti di terzi indipendenti, evidenze mirate; mai al posto della verifica diretta se il Cliente la vuole	ALLA FIRMA
e) iii)	Cooperazione piena alle ispezioni in loco di autorità, Lead Overseer, Cliente o terzo nominato	Art. 17.2	Accesso alla sede, ai sistemi in sola consultazione, ai documenti e alle persone	ALLA FIRMA
e) iv)	Perimetro, procedure e frequenza di audit e ispezioni	Art. 17.4	Perimetro: Servizio, infrastruttura, processi e subfornitori nei limiti dei loro contratti. Procedura: richiesta scritta (modulo 52), piano concordato, rapporto, piano di rimedio	ALLA FIRMA
f)	Strategia di uscita con un periodo di transizione adeguato obbligatorio: il fornitore continua il servizio e il Cliente migra o internalizza	Art. 18	Transizione fino a 12 mesi, alle condizioni economiche in vigore, con il Servizio pieno e l'assistenza al trasferimento (documento 56)	ALLA FIRMA
Par. 4	Clausole contrattuali standard delle autorità	Art. 26	Non risultano clausole standard UE adottate per DORA. Se le autorità le adottano, Trailgun adegua l'Allegato	ALLA FIRMA

Cliente microimpresa. In deroga alla lett. e), con un Cliente microimpresa (art. 3, punto 60) le parti possono concordare che l'audit sia delegato a un terzo indipendente nominato da Trailgun (art. 30, par. 3, ultimo comma). L'Allegato lo prevede come opzione del Cliente (art. 17.6), non come obbligo, e lascia al Cliente il diritto di chiedere in ogni momento informazioni e garanzie sull'operato del terzo.

06 · LIVELLO 2

La politica sui fornitori del Cliente: Reg. del. (UE) 2024/1773

Si applica ai soggetti tenuti all'art. 28, par. 2, quindi alle banche e non ai 106. Le banche lo usano come griglia della due diligence.

REG. 2024/1773	CHE COSA CHIEDE AL CLIENTE	CHE COSA FORNISCE TRAILGUN
Art. 1	Fattori di rischio: luogo del fornitore e della capogruppo, luogo dei dati, natura dei dati, vigilanza sul fornitore, concentrazione, trasferibilità	Sede in Italia [indirizzo]; capogruppo [se esiste]; dati e modelli nelle regioni UE di AWS (Germania, Irlanda); dati giudiziari e bancari; fornitore non vigilato; concentrazione su AWS (sezione 9); trasferibilità in formati aperti (sezione 13)
Art. 3	Politica riesaminata ogni anno; metodologia per la classificazione; contratti con obbligo di cooperazione con le autorità (par. 8, c) e accesso effettivo a dati e locali (par. 8, d)	Elementi per la classificazione (sezione 2); obbligo di cooperazione (All. art. 10) e diritti di accesso (All. art. 17)
Art. 4	Ciclo di vita dell'accordo, dalla scelta all'uscita	Questo documento segue le fasi: valutazione (sez. 2), contratto (sez. 4-5), monitoraggio (sez. 14), uscita (sez. 13)
Art. 5	Valutazione ex ante dei rischi: operativi, legali, TIC, reputazionali, dati personali, disponibilità, luoghi, concentrazione	Stato dei presidi (sezione 15) e Percorso (documento 12); Registro dei rischi ICT di Trailgun in sintesi su richiesta (documento 41); DPA e documento privacy; continuità (sezione 14)
Art. 6	Due diligence: reputazione, competenze, risorse, standard di sicurezza, organizzazione, subappaltatori, paesi terzi, consenso agli audit; condotta etica (lett. f); elementi di garanzia (par. 3)	Questionario precompilato (documento 13); risposte ai questionari entro 15 giorni lavorativi. Organizzazione dichiarata: accesso tecnico concentrato nel CEO, con i controlli compensativi della sezione 9. Elementi di garanzia: audit del Cliente, verbali delle prove di ripristino, politiche e registri, dichiarazione di applicabilità, rapporti AWS; sintesi del penetration test dal primo (Percorso R06)
Art. 7	Conflitti di interesse	Trailgun dichiara su richiesta i conflitti di interesse con il Cliente. Il cofondatore Alessandro Musella è avvocato e non ha ruoli esecutivi in Trailgun
Art. 8	Clausole dell'art. 30; audit e test anche congiunti; per le funzioni essenziali o importanti non basarsi nel tempo solo su certificazioni e rapporti, e verificarne il perimetro e il test di efficacia operativa	Allegato DORA completo; audit congiunti ammessi; diritti di verifica diretta mai sostituiti da certificazioni (All. art. 17.3)
Art. 9	Monitoraggio con indicatori di prestazione e di controllo; rapporti periodici del fornitore	Disponibilità misurata dalla sonda esterna, tempi dell'assistenza, incidenti, cambi di subfornitori, esiti delle prove, su richiesta; rapporti periodici in app e per email: Percorso R04
Art. 10	Piano di uscita documentato, riesaminato e testato, per interruzione persistente, servizio carente, risoluzione inattesa	Piano di uscita e di transizione per i tre scenari e per l'insolvenza di Trailgun (sezione 13, documento 56)

La gestione del rischio TIC del Cliente: Reg. del. (UE) 2024/1774

Le norme del regime ordinario che toccano il fornitore. Per il regime semplificato dei 106 valgono gli artt. 28-41, con gli stessi temi in forma più leggera.

REG. 2024/1774	TEMA	SITUAZIONE DI TRAILGUN	STATO
Art. 4	Date di fine supporto dei componenti	Node.js 24, Amazon Linux 2023 con immagine fissata e aggiornata ogni mese; immagine del proxy fissata a una versione; inventario degli asset (documento 42)	IN ESSERE
Art. 6	Cifratura a riposo, in transito, verso l'esterno	A riposo: dischi cifrati (EBS, AWS KMS, AES-256), copie cifrate in entrambe le regioni, archivio temporaneo cifrato. In transito: TLS 1.2 o superiore, HSTS di un anno. Nessuna cifratura applicativa dei database; chiavi gestite da Trailgun con la nuova piattaforma (R12)	IN ESSERE

REG. 2024/1774	TEMA	SITUAZIONE DI TRAILGUN	STATO
Art. 10	Gestione delle vulnerabilità del fornitore	Scansione di ogni immagine all'upload (ECR), delle dipendenze ogni settimana (Dependabot) e dei segreti a ogni verifica. Correzione: critica 72 ore, alta 7 giorni, media 30, bassa 90. Segnalazione responsabile pubblicata. Scansione esterna mensile: R05	IN ESSERE
Art. 11	Ruoli e responsabilità di sicurezza tra entità e fornitore	Ripartizione scritta nell'Allegato DORA: a Trailgun la piattaforma; al Cliente utenti, credenziali, visibilità dei clienti dello studio, dispositivi	ALLA FIRMA
Art. 12	Log: eventi, conservazione, protezione dalla manomissione	Log di accesso HTTP e applicativi 90 giorni; log di sicurezza e amministrazione (CloudTrail su tutte le regioni con convalida dell'integrità, sessioni di amministrazione) 12 mesi; registro delle attività per studio e registro degli accessi ai fascicoli penali	IN ESSERE
Art. 16	Test del software e, ove possibile, del codice sorgente	Verifica automatica obbligatoria prima di ogni rilascio, anche manuale: controllo dei tipi, test unitari e di interfaccia, scansione dei segreti, prova di ripristino. Branch di rilascio protetti. Codice consultabile in audit; deposito presso un terzo: R09	IN ESSERE
Artt. 20-21	Identità unica e autenticazione forte per gli accessi remoti e privilegiati	Utenti della piattaforma: secondo fattore TOTP obbligatorio. Il personale di Trailgun non accede ai sistemi del Cliente. Accessi amministrativi di Trailgun: credenziali temporanee (IAM Identity Center) e autenticazione a più fattori su ogni console	IN ESSERE
Art. 23	Notifiche del fornitore come fonte di rilevazione	Notifica entro 2 ore (sezione 10). Monitoraggio esterno ogni minuto e allarmi 24/7; GuardDuty	IN ESSERE
Art. 25	Test di continuità con i servizi dei fornitori e gli scenari di insolvenza del fornitore	Esiti delle prove di ripristino ai clienti DORA; partecipazione ai test del Cliente; piano di uscita per l'insolvenza di Trailgun (sezione 13, documento 56)	IN ESSERE

07 · REGISTRO DELLE INFORMAZIONI

I dati che Trailgun dà al Cliente per il registro

Art. 28, par. 3, DORA e Reg. es. (UE) 2024/2956. La Scheda per il Registro delle informazioni (documento 16, Excel) ha un foglio per modello, con ogni campo, il codice di colonna, il valore e chi lo compila.

7.1 Il codice identificativo di Trailgun

Per una persona giuridica il campo B_05.01.0020 ammette solo il LEI o l'EUID. Il LEI di Trailgun è [LEI]. Se Trailgun non appartiene a un gruppo, nel campo della capogruppo ultima (0110) si ripete il suo codice; l'assetto societario: [assetto societario].

CAMPO	NOME NEL MODELLO	VALORE PROPOSTO DA TRAILGUN
B_05.01.0010-0020	Identification code; type of code	[LEI] · LEI
B_05.01.0030-0040	Additional identification code; type	Partita IVA [...] · VAT number
B_05.01.0050-0060	Legal name; name in Latin alphabet	[Trailgun S.r.l.]
B_05.01.0070-0080	Type of person; country of headquarters	Legal person · IT
B_05.01.0090-0100	Currency; total annual expense	EUR · a cura del Cliente (spesa dell'ultimo anno)
B_05.01.0110-0120	Ultimate parent code; type	Stesso codice di 0010, salvo gruppo [...]
B_02.02.0060	Type of ICT services	S19 Cloud services: SaaS (il Cliente può aggiungere S06 Data analysis)
B_02.02.0100-0110	Notice periods (Cliente; fornitore)	90 giorni; 90 giorni, e per Trailgun solo per cessazione del Servizio per tutti i clienti, salvo il periodo di transizione

CAMPO	NOME NEL MODELLO	VALORE PROPOSTO DA TRAILGUN
B_02.02.0120	Country of the governing law	IT
B_02.02.0130	Country of provision of the ICT services	DE (infrastruttura a Francoforte); gestione e assistenza dall'Italia (IT)
B_02.02.0140-0150	Storage of data; location of data at rest	Yes · DE (copie di sicurezza in IE)
B_02.02.0160	Location of management of the data (processing)	DE per conservazione, OCR e trascrizione; modelli ed embeddings su Amazon Bedrock nella regione di Francoforte (UE)
B_02.02.0170	Sensitiveness of the data	High (dati giudiziari anche penali, segreto bancario e professionale)
B_02.02.0180	Level of reliance	A cura del Cliente (sezione 2)
B_05.02	ICT service supply chain, con il rango	Trailgun rango 1; subfornitori che sostengono il servizio rango 2 e 3 (sezione 8)
B_07.01.0050	Substitutability	Proposta: medium complexity. Dati esportabili in formati aperti; gli elaborati sono DOCX e PDF
B_07.01.0070	Date of the last audit on the provider	Data dell'ultimo audit del Cliente su Trailgun, se svolto; il primo penetration test indipendente è la tappa R06 del Percorso
B_07.01.0080-0090	Exit plan; possibility of reintegration	Piano di uscita e di transizione di Trailgun (documento 56) per il piano di uscita del Cliente; reintegrazione: valuta il Cliente (ritorno alla redazione manuale)
B_06.01.0080-0090	RTO e RPO della funzione	Del Cliente. Per essere compatibili con Trailgun: RTO non inferiore a 8 ore e RPO non inferiore a 24 ore, o una procedura alternativa (sezione 14)

Aggiornamenti. Trailgun aggiorna la Scheda a ogni cambiamento dei dati e dei subfornitori, con lo stesso preavviso dei cambiamenti, e la rimanda al Cliente su richiesta prima della sua segnalazione annuale. I codici di colonna seguono l'Allegato I del Reg. es. 2024/2956: il Cliente li verifica sulla versione dei modelli in uso presso la propria autorità.

08 · SUBFORNITURA

La catena di subfornitura

Art. 29, par. 2, DORA e Reg. del. (UE) 2025/532. Rango secondo il modello B_05.02: 1 è Trailgun, 2 i suoi subfornitori diretti, 3 i loro. La stessa catena è nel Registro dei subfornitori (documento 15) e su https://trailgun.ai/subprocessors.

RANGO	FORNITORE E SEDE	SERVIZIO	DATI E LUOGO	SOSTIENE IL SERVIZIO	GARANZIE
2	**Amazon Web Services EMEA SARL**, Lussemburgo; capogruppo Amazon.com, Inc., Stati Uniti	Infrastruttura, conservazione, login (Cognito), email di sistema (SES), OCR (Textract), trascrizione (Transcribe), copie di sicurezza, log e rilevazione; esecuzione dei modelli Claude e degli embeddings Amazon Titan (Bedrock)	Tutti i dati; Germania, copie in Irlanda; modelli nelle regioni UE	Sì	DPA FIRMATO opt-out dei servizi di IA
3	**Anthropic**, Stati Uniti	Fornisce ad AWS i modelli Claude eseguiti su Bedrock	Nessun dato di Trailgun: il modello gira su AWS	Sì (modello)	condizioni di Amazon Bedrock
2	**Plus Five Five, Inc. (Resend)**, Stati Uniti	Email in uscita, risposte e caselle di ingresso delle pratiche	Indirizzi, testi, allegati delle risposte; invio e ricezione su AWS in Irlanda	In parte (canale email)	DPA FIRMATO Data Privacy Framework
2	**Openapi S.p.A.**, Italia, con **Namirial S.p.A.** (rango 3)	Firma qualificata e visure, solo su richiesta	PDF da firmare, dati del firmatario e dell'impresa; Italia	No (accessorio)	DPA FIRMATO
2	**Wolters Kluwer Italia S.r.l.** (One LEGALE), Italia	Banca dati giuridica per ricerca fonti e verifica giurisprudenziale	Stringhe di ricerca senza dati delle pratiche; Italia	No (accessorio)	DPA FIRMATO

RANGO	FORNITORE E SEDE	SERVIZIO	DATI E LUOGO	SOSTIENE IL SERVIZIO	GARANZIE
2	**Hoss Inc. (DocuPipe)**, Stati Uniti	OCR di riserva per i file che Textract non legge, solo per lo studio che lo accende	Il singolo file; Stati Uniti	No (opzione spenta di default)	DPA FIRMATO clausole tipo

Non ricevono dati delle pratiche: Telegram e Twilio (notifiche agli utenti che le scelgono, solo avviso e link); Stripe (pagamenti dello studio, titolare autonomo); Microsoft (nella revisione in Word il file va dal browser dell'avvocato al suo OneDrive o SharePoint); GitHub, Let's Encrypt, Docker Hub e npm (catena di fornitura del software); Google Workspace (caselle delle persone di Trailgun).

Reg. del. (UE) 2025/532, articolo per articolo

REG. 2025/532	REQUISITO	COME LO SODDISFA TRAILGUN
Art. 3	Il fornitore sa selezionare e valutare i subappaltatori, identificarli tutti, ha contratti che consentono al Cliente di rispettare DORA, ottiene gli stessi diritti di accesso e ispezione, ha risorse per monitorarli	Valutazione prima dell'ingaggio e ogni anno (procedura 29), con il Registro dei subfornitori (documento 15: DPA, certificazioni, regioni, garanzie di trasferimento). Catena dichiarata per intero. Contratti sul trattamento dei dati con ogni fornitore in essere. Per AWS i diritti di verifica si esercitano secondo il programma di garanzia di AWS (rapporti di AWS Artifact: ISO 27001, 27017, 27018, SOC 2, C5): AWS non concede audit individuali ai clienti dei suoi clienti, ed è sottoposta come fornitore critico alla sorveglianza del Lead Overseer. Il Cliente ne tiene conto nella sua valutazione
Art. 4	Contenuto del contratto: responsabilità del fornitore, monitoraggio, rapporti, luogo dei dati, continuità lungo la catena, piani di emergenza e standard di sicurezza, diritti dell'art. 30, par. 3, lett. e), notifica dei cambiamenti	Art. 19 dell'Allegato DORA: Trailgun risponde dei subfornitori come di sé stessa, li monitora, ne riferisce al Cliente, indica il luogo dei dati di ciascuno e porta nei subcontratti gli obblighi pertinenti, nei limiti dei contratti standard degli hyperscaler
Art. 5	Cambiamenti rilevanti: informativa con anticipo, termine ragionevole per approvare od opporsi, attuazione solo dopo approvazione o mancata opposizione	Preavviso di 60 giorni per le funzioni essenziali o importanti, 30 negli altri casi. Il cambiamento si attua solo dopo l'approvazione espressa o la scadenza del termine senza opposizione, mai finché un'opposizione è pendente. Per i Clienti DORA questa regola sostituisce l'art. 12.5 del DPA. Sostituzione urgente solo per sicurezza o cessazione del fornitore, comunicata entro 72 ore, con diritto di opposizione
Art. 6	Risoluzione se il fornitore attua cambiamenti contestati o non approvati, o subappalta servizi non ammessi	Causa di risoluzione dell'Allegato (art. 11); in più, recesso senza penali con rimborso della quota pagata e non goduta se l'opposizione non si risolve in 30 giorni

09 · CONCENTRAZIONE

Rischio di concentrazione: AWS e le altre dipendenze

L'infrastruttura e i modelli di Trailgun sono su AWS; alcune funzioni accessorie usano altri fornitori (sezione 8). Una catena corta, con i dati nel perimetro AWS dell'Unione, ha come contropartita la dipendenza da un solo fornitore principale. Il Cliente lo deve sapere per l'art. 29, par. 1.

9.1 I fatti

- Un'istanza EC2 per ambiente, nella regione di Francoforte, in un account AWS dedicato e intestato a Trailgun; dati in due database SQLite e in file su un disco cifrato dedicato.
- Copie giornaliere del disco conservate a Francoforte e copiate cifrate in Irlanda. Infrastruttura descritta come codice (AWS CDK) e ricostruibile; runbook di ripristino scritto e provato ogni trimestre.
- Pila applicativa, registro delle immagini, segreti e pool di login stanno a Francoforte e si ricreano in Irlanda dall'infrastruttura come codice; procedura regionale provata: Percorso R03, R10.
- Amazon Web Services EMEA SARL è un fornitore critico designato il 18/11/2025 ed è quindi già sotto la sorveglianza del Lead Overseer. Se il Cliente usa AWS direttamente o tramite altri fornitori, la dipendenza da AWS si somma.

RISCHIO	MITIGAZIONE IN ESSERE	PERCORSO
Guasto di istanza, disco o zona	Ripristino dalla copia giornaliera con il runbook provato: RTO 8 ore, RPO 24 ore; sonda e allarmi 24/7	R01, R12, R14
Perdita della regione di Francoforte	Copie cifrate in Irlanda; infrastruttura come codice	R03, R10
Cancellazione o cifratura malevola delle copie	Credenziali amministrative temporanee con MFA; CloudTrail 12 mesi; GuardDuty; copie in due regioni	R11
Uscita da AWS o condizioni inaccettabili	Container standard, infrastruttura come codice, dati in formati aperti: la piattaforma è ricostruibile altrove. Trailgun non promette un'architettura su più cloud	R09
Fornitore unico dei modelli	Modelli Claude su Bedrock, disponibili in più regioni UE di AWS; gli elaborati già prodotti restano consultabili; il modello si configura dal pannello della piattaforma e un modello diverso richiede una nuova validazione della qualità degli elaborati	–
Persona chiave	Accesso tecnico concentrato nel CEO, bilanciato da: runbook scritti e provati, infrastruttura come codice, accesso di emergenza con un depositario (documento 11), credenziali temporanee, CloudTrail, revisione trimestrale degli accessi	R09, R13

10 · INCIDENTI

Incidenti: i tempi di Trailgun dentro quelli del Cliente

Il Cliente segnala gli incidenti gravi all'autorità nei termini dell'art. 5 del Reg. del. (UE) 2025/301. I tempi di Trailgun sono più stretti, per lasciargli margine. Sono impegni contrattuali, non obblighi di legge del fornitore. Procedura 25; modelli di notifica 51.

FASE	OBBLIGO DEL CLIENTE	IMPEGNO DI TRAILGUN	MARGINE
Notifica iniziale	Entro 4 ore dalla classificazione come grave e comunque entro 24 ore dalla conoscenza	Entro 2 ore da quando Trailgun viene a conoscenza di un incidente TIC che incide o può incidere sul Servizio o sui dati del Cliente: email alla casella di sicurezza del Cliente e telefonata al referente	Il Cliente riceve gli elementi per classificare entro la seconda ora
Aggiornamenti	–	Almeno ogni 24 ore fino alla chiusura e a ogni cambiamento rilevante	–
Relazione intermedia	Entro 72 ore dalla notifica iniziale	Entro 48 ore dalla notifica iniziale di Trailgun, con i dati per i moduli del Reg. es. 2025/302	Almeno 24 ore
Relazione finale	Entro 1 mese dall'ultima relazione intermedia	Entro 20 giorni dalla chiusura dell'incidente, e comunque in tempo per la relazione finale del Cliente	Circa 10 giorni
Minacce informatiche significative	Notifica volontaria (art. 19, par. 2)	Comunicazione entro 24 ore delle minacce che possono riguardare il Cliente	–
Violazione di dati personali	Notifica al Garante entro 72 ore, ove possibile (art. 33 GDPR)	Entro 24 ore al Titolare; per il Cliente DORA vale anche la notifica di 2 ore	Almeno 48 ore

10.1 Che cosa contiene la notifica di Trailgun

Gli elementi che servono al Cliente per classificare secondo il Reg. del. 2024/1772 e compilare i moduli del Reg. es. 2025/302, per quanto noti e poi per fasi:

- data e ora di rilevazione e di inizio dell'incidente; servizi e verticali colpiti; durata e tempo di inattività;
- dati coinvolti e se c'è stato un accesso non autorizzato riuscito; numero di utenti e pratiche del Cliente toccati;
- origine dell'incidente, anche presso un subfornitore, e rango nella catena;
- causa, impatto, misure di contenimento, tempi stimati di ripristino, indicatori di compromissione utili al Cliente.

Per il Reg. del. 2024/1772 un incidente che colpisce servizi critici è grave se c'è un accesso malevolo non autorizzato riuscito che può portare a perdite di dati, oppure se si superano due o più soglie, fra cui l'inattività oltre 2 ore di un servizio che sostiene una funzione essenziale o importante (artt. 8 e 9). Per questo la notifica parte entro 2 ore anche senza diagnosi completa.

10.2 Come Trailgun rileva e gestisce gli incidenti

- Monitoraggio esterno ogni minuto e allarmi 24/7 su salute, disco, CPU, memoria, errori e certificati, che raggiungono il reperibile.
- CloudTrail su tutte le regioni con convalida dell'integrità, GuardDuty e registrazione delle sessioni di amministrazione, conservati 12 mesi.
- Procedura di risposta agli incidenti (documento 25) con tre livelli (grave, significativo, minore) allineati ai criteri del Reg. del. 2024/1772; registro degli incidenti. Nel registro è annotato il riavvio di produzione fallito del 21/10/2026, un incidente operativo di disponibilità senza perdita né esposizione di dati.
- Casella security@trailgun.ai presidiata; per la priorità 1 anche il numero di reperibilità 24/7 `[+39 ...]`.

Trailgun assiste il Cliente in ogni incidente legato al Servizio senza costi aggiuntivi (art. 30, par. 2, lett. f). Il Contratto non prevede l'esternalizzazione della segnalazione all'autorità (art. 19, par. 5): la segnalazione resta del Cliente, Trailgun gli dà i dati.

Il Reg. del. 2025/301 consente di presentare entro mezzogiorno del giorno lavorativo successivo le segnalazioni che scadono nel fine settimana o in un festivo, salvo per gli enti creditizi e per i soggetti essenziali o importanti NIS2. I tempi di Trailgun valgono tutti i giorni dell'anno.

11 · TEST

Test di resilienza e TLPT

Il programma di test del Cliente (artt. 24-25) comprende i sistemi TIC che sostengono funzioni essenziali o importanti, anche se di terzi. Ecco che cosa fa Trailgun e che cosa dà al Cliente.

TEST	FREQUENZA	CHE COSA RICEVE IL CLIENTE	STATO
Scansione delle immagini (ECR)	A ogni immagine	Esiti in audit	IN ESSERE
Dipendenze (Dependabot) e **segreti** (gitleaks)	Ogni settimana; a ogni verifica	Esiti in audit	IN ESSERE
Prova automatica di ripristino	A ogni verifica della CI	Esiti in audit	IN ESSERE
Prova di ripristino sullo snapshot reale	Trimestrale, in ambiente isolato	Verbale con l'RTO misurato, sempre ai clienti DORA	IN ESSERE
Piano di continuità	Prova annuale	Piano (documento 11) ed esito della prova	IN ESSERE
Scansione esterna dell'applicazione	Mensile	Sintesi su richiesta	PERCORSO R05
Penetration test indipendente	Annuale e dopo ogni cambiamento rilevante dell'architettura	Sintesi dei risultati e piano di rimedio, sotto riservatezza	PERCORSO R06
Prova di ripristino regionale	Annuale	Esito	PERCORSO R10
Test del Cliente (artt. 24-25)	Secondo il programma del Cliente	Partecipazione e cooperazione, con perimetro, finestre e regole d'ingaggio concordati per iscritto	ALLA FIRMA
TLPT del Cliente (art. 26)	Almeno ogni 3 anni, per le entità individuate dall'autorità	Partecipazione piena, anche al test congiunto	ALLA FIRMA

11.1 Come Trailgun partecipa a un TLPT

- **Chi lo fa.** Il TLPT si applica solo alle entità individuate dall'autorità (art. 26, par. 1 e 8). Non si applica ai 106, perché l'art. 6 del D.Lgs. 23/2025 non richiama gli artt. 26-27, né ai soggetti del regime semplificato e alle microimprese.
- **Perimetro.** Se Trailgun rientra nel perimetro del test del Cliente (art. 26, par. 2-3), partecipa e coopera, anche ai controlli di rischio durante il test (par. 5).
- **Test congiunto.** Poiché la piattaforma è condivisa fra clienti, se un test diretto può nuocere agli altri clienti Trailgun può incaricare direttamente un tester esterno, sotto la direzione di un'entità designata, per un test congiunto di più entità finanziarie (art. 26, par. 4).
- **Squadre.** Il personale di Trailgun può far parte del «control team» e del «blue team» (art. 1 del Reg. del. (UE) 2025/1190).
- **Regole.** Perimetro, scenari, finestre, contatti di emergenza, criteri di sospensione e trattamento dei risultati si concordano per iscritto prima del test. I risultati che riguardano Trailgun restano riservati fra le parti e le autorità.

12 · AUDIT

Accesso, ispezione e audit, anche della Banca d'Italia

Art. 28, par. 6, e art. 30, par. 3, lett. e), DORA; art. 8 D.Lgs. 23/2025; art. 114.11 TUB per i gestori di crediti in sofferenza. Modulo di richiesta: documento 52.

TIPO	FREQUENZA	PREAVVISO	MODALITÀ
Audit ordinario	1 all'anno	30 giorni	In orario lavorativo, fino a 2 giorni in loco, senza compromettere gli altri clienti; prima i documenti e le certificazioni disponibili
Audit straordinario	Dopo un incidente grave o su richiesta di un'autorità	5 giorni lavorativi	Come sopra, sul perimetro dell'evento
Funzioni essenziali o importanti e autorità	Illimitati	Quello fissato dall'autorità; per il Cliente, concordato secondo l'urgenza	Accesso, ispezione, audit, copia della documentazione, anche in loco; audit congiunti ammessi
Questionari	1 all'anno senza costi; oltre, su accordo	Risposta entro 15 giorni lavorativi	Questionari del Cliente o standard di mercato

12.1 Banca d'Italia e altre autorità

Le autorità DORA possono effettuare «accessi e ispezioni» presso i fornitori terzi di servizi TIC a supporto di funzioni essenziali o importanti, «convocare gli amministratori, i sindaci e il personale» e chiedere informazioni e documenti (art. 8, c. 1-2, D.Lgs. 23/2025). Per i gestori di crediti in sofferenza la Banca d'Italia può convocare gli amministratori di chi riceve funzioni esternalizzate ed effettuare ispezioni (art. 114.11, c. 7-8, TUB).

Trailgun si obbliga verso il Cliente a cooperare pienamente: accesso alla sede [indirizzo], ai sistemi in sola consultazione, ai documenti e alle persone; risposta alle richieste nei termini fissati dall'autorità. La mancata collaborazione esporrebbe Trailgun alle sanzioni dell'art. 144, c. 8-bis, TUB.

12.2 Che cosa si può verificare

- Configurazione dell'infrastruttura come codice: rete, cifratura dei dischi, politiche delle copie, ruoli e permessi; registri di CloudTrail.
- Configurazione dell'autenticazione degli utenti (secondo fattore obbligatorio, politica delle password) e degli accessi amministrativi.
- Esiti della verifica automatica che precede ogni rilascio; Registro dei cambiamenti (documento 45).
- Registro delle attività dello studio, registro degli accessi ai fascicoli penali, registro degli accessi del personale.
- Rapporti di AWS da AWS Artifact; contratti con i subfornitori nei limiti della loro riservatezza; Registro dei subfornitori.
- Politiche P01-P17, procedure 20-31, registri 40-45, piano di continuità, verbali delle prove di ripristino; sintesi del penetration test dal primo (R06).

Limiti a tutela degli altri clienti. Nessun audit dà accesso ai dati di altri clienti. Dove un'attività rischia di toccarli, Trailgun propone un livello alternativo di garanzia (audit congiunto, rapporto di un terzo indipendente, evidenza mirata), ferma la facoltà del Cliente e dell'autorità di svolgere la verifica diretta. Ciascuna parte sostiene i propri costi.

13 · USCITA

Strategia di uscita e piano di transizione

Art. 28, par. 8, e art. 30, par. 3, lett. f), DORA; art. 10 del Reg. del. 2024/1773; artt. 25 e 29 del Regolamento (UE) 2023/2854 (Data Act). Il piano completo è il documento 56; la procedura operativa è la 28.

13.1 Quando si attiva

1. **Cessazione ordinaria**: scadenza, disdetta o recesso secondo l'art. 20 delle Condizioni generali.
2. **Risoluzione**: nei casi dell'art. 28, par. 7, DORA, per i cambi di subfornitori contestati o per inadempimento.
3. **Interruzione persistente o servizio carente**, secondo il piano di uscita del Cliente (art. 10 del Reg. del. 2024/1773).
4. **Decisione dell'autorità** che non possa vigilare efficacemente sul servizio (art. 28, par. 7, lett. d).
5. **Insolvenza o cessazione dell'attività di Trailgun**, o cessazione del Servizio senza subentro.

FASE	DURATA	CHE COSA FA TRAILGUN
Avvio	Alla richiesta del Cliente	Nomina un referente per l'uscita; concorda con il Cliente il piano di transizione: perimetro, calendario, formati, destinatario dei dati, criteri di completamento
Transizione	Standard 30 giorni inclusi nel canone; per i clienti DORA fino a 12 mesi, alle condizioni economiche in vigore	Continua a prestare il Servizio con gli stessi livelli; esporta i dati; documenta formati e struttura; risponde alle domande tecniche del nuovo fornitore o del Cliente che internalizza; nessuna nuova funzione obbligatoria
Esportazione complessiva	Entro 10 giorni lavorativi dalla richiesta	Archivio ZIP cifrato con documenti originali, elaborati in DOCX e PDF/A, testi estratti in TXT, dati strutturati in JSON e CSV, registro delle attività e degli accessi penali in CSV, indice dei file con impronte SHA-256. Consegna con link temporaneo cifrato o via API, con estrazione assistita da Trailgun e certificato di restituzione (documento 53). In autonomia dall'app: Percorso R02
Accesso dopo la cessazione	30 giorni	Sola lettura con esportazione, pratica per pratica (archivio originale, faldone, pacchetto per il deposito)
Cancellazione	Entro i 30 giorni successivi	Cancella tutti i dati dello studio, compresi testi estratti, cache OCR, conversazioni con gli agenti, indici, registri delle lavorazioni e utenti; conferma scritta entro 5 giorni lavorativi con il certificato di cancellazione (documento 54)
Copie di sicurezza	Entro 14 giorni dalla cancellazione	Tutte le copie, comprese quelle fatte prima dei rilasci, escono per rotazione
In tutto	Al massimo 74 giorni dalla cessazione (30 + 30 + 14)	Per i clienti DORA i termini decorrono dalla fine del periodo di transizione. Restano solo i dati di fatturazione dello studio, 10 anni (art. 2220 c.c.)

13.2 Data Act

Nella misura in cui il Servizio è un «servizio di trattamento dei dati» (art. 2, punto 8, Reg. (UE) 2023/2854), il Cliente può chiedere il passaggio ad altro fornitore o l'esportazione con un preavviso massimo di 2 mesi (art. 25, lett. d), che prevale sul preavviso di 90 giorni delle Condizioni generali. Il periodo di transizione è di 30 giorni (lett. a), prolungabile; il periodo per recuperare i dati è di almeno 30 giorni (lett. g). Fino al 12/01/2027 si possono addebitare solo costi di passaggio ridotti, non superiori ai costi diretti; dal 12/01/2027 nessun costo di passaggio (art. 29). Per i clienti DORA la transizione può durare di più, fino a 12 mesi, su richiesta del Cliente.

13.3 Deposito del codice e insolvenza

Il deposito del codice sorgente e delle istruzioni per ricostruire la piattaforma presso un agente terzo, aggiornato ogni trimestre, è la tappa R09 del Percorso; le condizioni sono nel term sheet del documento 57. Condizioni di rilascio al Cliente beneficiario: insolvenza di Trailgun, cessazione dell'attività o del Servizio senza subentro. Agente: [agente di escrow]. In ogni momento il Cliente può esportare i propri dati.

13.4 Sostituibilità e reintegrazione

Gli elaborati sono documenti Word e PDF che restano al Cliente; i dati strutturati escono in JSON e CSV con le fonti. Per reintegrare il lavoro il Cliente torna alla redazione da parte dei suoi avvocati o passa a un altro fornitore: la scelta delle alternative (B_07.01.0110-0120) è sua. Per provare il piano di uscita il Cliente può chiedere in ogni momento un'esportazione di prova.

14 · CONTINUITÀ

Continuità operativa e livelli di servizio

I livelli in vigore dalla firma. Il testo contrattuale è l'Accordo sul livello di servizio (documento 55); l'evoluzione è nel Percorso (documento 12).

PARAMETRO	IMPEGNO DALLA FIRMA	EVOLUZIONE
RPO	24 ore (copia giornaliera alle 02:00 UTC; nei giorni di rilascio la copia pre-rilascio lo accorcia)	R01, R14
RTO istanza, disco o zona	8 ore di calendario dalla dichiarazione dell'incidente, misurato nella prova trimestrale	R14
RTO perdita della regione	Copie in Irlanda; ricostruzione dall'infrastruttura come codice	R03, R14
Periodo massimo tollerabile	5 giorni lavorativi	–
Copie	Ogni 24 ore e prima di ogni rilascio; 14 giorni ciascuna; Germania e Irlanda, cifrate	R01, R11, R12
Disponibilità 24/7	99,5 % mensile	R14
Disponibilità nei giorni lavorativi 08:00-20:00	99,8 % mensile	R14

14.1 Come si garantiscono

- Un'istanza per ambiente, ricostruibile dall'infrastruttura come codice. Un rilascio riavvia il server: lo script di rilascio si rifiuta se ci sono lavorazioni del modulo in corso, quelle in coda ripartono da sole.
- Runbook di ripristino scritto (procedura 30); prova trimestrale sullo snapshot reale con verbale e RTO misurato (programma 31); prova automatica a ogni verifica della CI.
- Tutte le copie, comprese quelle fatte prima dei rilasci, scadono a 14 giorni.
- La disponibilità è misurata ogni minuto da una sonda esterna sul controllo di salute e sull'avvio di una lavorazione.
- Piano di continuità operativa e di ripristino adottato (documento 11), rivisto e provato ogni anno.
- La nuova piattaforma su più zone di disponibilità, con container senza stato dietro un bilanciatore con WAF, database gestito con ripristino a un istante, file su S3 con versioni e chiavi di Trailgun e lavorazioni in una coda che sopravvive ai rilasci, è la tappa R12; i livelli che ne derivano sono la tappa R14.

Per il Cliente: gli elaborati già scaricati restano utilizzabili e il deposito resta sempre all'avvocato. L'RTO e l'RPO che il Cliente scrive per la propria funzione (B_06.01) devono essere compatibili con questi valori o avere una procedura alternativa.

14.2 Manutenzione, crediti di servizio e assistenza

Manutenzione programmata con almeno 48 ore di preavviso, tra le 20:00 e le 07:00 o nel fine settimana, al massimo 8 ore al mese; mai nella finestra dei giorni lavorativi 08:00-20:00. Rilasci ordinari sotto i 2 minuti e solo senza lavorazioni del modulo in corso; una lavorazione interrotta si riavvia senza costi. Interventi urgenti di sicurezza anche senza preavviso, comunicati appena possibile.

Crediti di servizio sul canone mensile: 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 %. Da chiedere entro 30 giorni dalla fine del mese; tetto annuo del 30 % dei corrispettivi.

PRIORITÀ	ESEMPIO	PRESA IN CARICO	SOLUZIONE O AGGIRAMENTO	AGGIORNAMENTI
1 · Bloccante	Piattaforma inaccessibile; sospetto incidente sui dati	1 ora, 24/7	4 ore	Ogni 2 ore fino al ripristino
2 · Grave	Un verticale non completa le lavorazioni	4 ore lavorative	1 giorno lavorativo	Ogni giorno lavorativo
3 · Ordinaria	Errore ricorrente in un elaborato; funzione degradata	1 giorno lavorativo	5 giorni lavorativi	Alla soluzione

PRIORITÀ	ESEMPIO	PRESA IN CARICO	SOLUZIONE O AGGIRAMENTO	AGGIORNAMENTI
4 · Richiesta	Domande d'uso, nuove esigenze	2 giorni lavorativi	Pianificazione concordata	–

15 · STATO E PERCORSO

Che cosa è in essere, e il Percorso

Lo stato al 01/12/2026. Ogni presidio ha la sua evidenza, che Trailgun mostra in audit. Le tappe successive sono nel documento 12, con le date; l'Allegato DORA le rende vincolanti.

15.1 In essere, con evidenza

- Infrastruttura AWS a Francoforte in un account dedicato, descritta come codice; ambienti di sviluppo, collaudo e produzione separati; fuori produzione i servizi esterni sono simulati.
- Modelli Claude ed embeddings su Amazon Bedrock nelle regioni UE; opt-out dei servizi di IA di AWS; nessun addestramento sui dati dei clienti.
- Dischi cifrati; HSTS e intestazioni di sicurezza; archivio temporaneo per OCR e trascrizione cifrato, non pubblico, cancellato a fine analisi e comunque entro 1 giorno.
- Nessuna porta SSH; amministrazione con AWS Systems Manager e sessioni registrate; credenziali temporanee con MFA su ogni console; segreti in Parameter Store, ruotati ogni anno, con scansione a ogni verifica.
- Login solo su invito con secondo fattore TOTP obbligatorio per tutti; token verificato a ogni richiesta; ruoli admin, membro, operator e viewer imposti dal server.
- Isolamento fra studi e visibilità per cliente con un unico controllo, coperto da test; cache OCR per studio; chiavi API conservate solo come hash; webhook firmati.
- Fascicoli penali: nessun embedding e registro degli accessi consultabile dallo studio.
- Log di accesso e applicativi 90 giorni; CloudTrail e log di amministrazione 12 mesi; GuardDuty; sonda esterna e allarmi 24/7.
- Copia giornaliera, 14 conservate, copia cifrata in Irlanda; copie pre-rilascio a 14 giorni; prova di ripristino trimestrale e nella CI.
- Branch protetti; rilasci con verifica obbligatoria, anche manuali; container non root; immagini fissate e aggiornate; scansione delle immagini e delle dipendenze.
- Piano di continuità; procedura incidenti a tre livelli; registro degli incidenti e delle violazioni; registro dei fornitori e valutazione annuale; elenco pubblico dei subfornitori; registro degli accessi del personale; DPA firmati con i subfornitori.
- Cancellazione completa a fine contratto con certificato; notifiche esterne senza dati delle pratiche; ricerche giuridiche senza dati delle pratiche; marcatura dei contenuti generati con l'IA.
- Politiche P01-P17 approvate; formazione registrata; verifica dei precedenti per chi accede alla produzione; revisione trimestrale degli accessi; polizze cyber e RC professionale.

TAPPA	PERCORSO DI CERTIFICAZIONE E PIATTAFORMA (DATE NEL DOCUMENTO 12)
R01	RPO 4 ore: snapshot ogni 4 ore conservati 7 giorni
R02	Esportazione complessiva in autonomia dall'app (fino ad allora estrazione assistita negli stessi 10 giorni lavorativi)
R03	Ripristino regionale in Irlanda: procedura scritta e provata, poi RTO regionale
R04	Rapporto di servizio mensile in app e trimestrale per email
R05	Scansione esterna mensile dell'applicazione
R06	Primo penetration test indipendente, poi ogni anno; sintesi e piano di rimedio ai clienti
R07, R08	Gap assessment ISO/IEC 27001:2022; SGSI operativo con dichiarazione di applicabilità definitiva
R09	Deposito del codice presso un agente di escrow, aggiornato ogni trimestre
R10, R11	Prima prova completa di ripristino regionale, poi ogni anno; copie protette dalla cancellazione per 7 giorni

TAPPA	PERCORSO DI CERTIFICAZIONE E PIATTAFORMA (DATE NEL DOCUMENTO 12)
R12	Nuova piattaforma su più zone (ECS Fargate, ALB con WAF, Aurora PostgreSQL con PITR, S3 con versioning, chiavi KMS di Trailgun, AWS Backup)
R13	Responsabile della sicurezza dedicato
R14	Nuovi livelli di servizio dopo la nuova piattaforma
R15, R16	Audit di stage 1; certificato ISO/IEC 27001:2022 (piattaforma Trailgun e processi di supporto)
R17	Valutazione ISO/IEC 42001 (obiettivo, non impegno)

15.2 Che cosa Trailgun non dichiara

- Nessuna certificazione propria (ISO/IEC 27001, SOC 2 o altre): le certificazioni che coprono il servizio sono quelle di AWS; quella di Trailgun è la tappa R16.
- Nessun penetration test indipendente finora: il primo è la tappa R06.
- Nessuna ridondanza su più zone di disponibilità finché non arriva la nuova piattaforma (R12).
- Nessun responsabile della sicurezza dedicato finora: il ruolo è del CEO fino alla tappa R13.

16 · CONTATTI E RIFERIMENTI

Contatti, documenti collegati e norme citate

RUOLO	CONTATTO
Legale rappresentante e referente contrattuale	Franco Puppo, CEO, [email]
Responsabile della sicurezza	Franco Puppo, CEO
Sicurezza e incidenti	security@trailgun.ai; priorità 1: [+39 ...], 24/7
Privacy	privacy@trailgun.ai
DPO	[DPO esterno: nome o società], dpo@[...]
Assistenza	In app (le cuffie nella barra in alto: agente e ticket) e info@trailgun.ai; giorni lavorativi 09:00-18:00
Società	[Trailgun S.r.l.]; sede [indirizzo]; P.IVA [...]; PEC [...]; LEI [...]

DOCUMENTO COLLEGATO	CONTENUTO
18 Allegato DORA al contratto	Le clausole degli artt. 28-30, firmabili; Sezione B per le funzioni essenziali o importanti
16 Scheda per il Registro delle informazioni	I campi dei modelli B_02-B_07 che riguardano Trailgun
17 Mappa DORA · 48 Mappa EBA	Requisito per requisito, con clausola, documento ed evidenza
55 SLA · 56 Piano di uscita · 57 Escrow	Livelli di servizio; uscita e transizione; deposito del codice
11 Continuità · 25 Incidenti · 51 Modelli di notifica	Piano di continuità; procedura di risposta; moduli per le notifiche
12 Percorso	Le tappe R01-R17 con le date e le evidenze

NORMA	ESTREMI
DORA	Regolamento (UE) 2022/2554 del 14/12/2022, GUUE L 333 del 27/12/2022; si applica dal 17/01/2025
Gestione del rischio TIC	Reg. del. (UE) 2024/1774 del 13/03/2024, GUUE del 25/06/2024
Politica sui fornitori	Reg. del. (UE) 2024/1773 del 13/03/2024, GUUE del 25/06/2024
Registro delle informazioni	Reg. es. (UE) 2024/2956 del 29/11/2024, GUUE del 02/12/2024

NORMA	ESTREMI
Classificazione degli incidenti	Reg. del. (UE) 2024/1772 del 13/03/2024, GUUE del 25/06/2024
Segnalazione degli incidenti	Reg. del. (UE) 2025/301 e Reg. es. (UE) 2025/302 del 23/10/2024, GUUE del 20/02/2025
Subappalto	Reg. del. (UE) 2025/532 del 24/03/2025, GUUE del 02/07/2025
TLPT	Reg. del. (UE) 2025/1190 del 13/02/2025, GUUE del 18/06/2025
Fornitori critici	Reg. del. (UE) 2024/1502 del 22/02/2024, GUUE del 30/05/2024; elenco delle AEV del 18/11/2025
Attuazione italiana	D.Lgs. 10 marzo 2025, n. 23, GU n. 58 dell'11/03/2025: artt. 6, 8, 10 (art. 144, c. 8-bis e 8-ter, TUB), 15, 17
Banca d'Italia	Documento di consultazione del 30/09/2026 sulle disposizioni per gli intermediari ex art. 106 TUB (Circolare n. 288/2015, Titolo III, Cap. 1, Sez. V)
Crediti in sofferenza	D.Lgs. 30 luglio 2024, n. 116 (artt. 114.1-114.14 TUB)
Data Act	Regolamento (UE) 2023/2854 del 13/12/2023, si applica dal 12/09/2025: artt. 2, 25, 29
NIS2	Direttiva (UE) 2022/2555; D.Lgs. 4 settembre 2024, n. 138
GDPR	Regolamento (UE) 2016/679: artt. 28 e 33

ENGLISH SUMMARY

Trailgun as an ICT third-party service provider under DORA

A one-stop summary for international banks and their vendor-risk teams. The Italian text prevails. Status at 1 December 2026; every control listed is in place with evidence for audit, and future milestones carry a roadmap code (R01-R17) dated in document 12.

EN.1 Scope and role

- **Who is subject.** DORA (Regulation (EU) 2022/2554) binds the client, the financial entity. Trailgun is an «ICT third-party service provider» (Art. 3(19)) delivering an ICT service (Art. 3(21)); register type S19, Cloud SaaS. Italian Art. 106 TUB intermediaries apply Arts. 28 (except para. 2), 29 and 30(1)-(4) from 1 January 2027 (Legislative Decree 23/2025, Arts. 6 and 17), under the simplified regime, without TLPT.
- **Not a CTPP.** Trailgun is far below the Art. 31 criteria and the thresholds of Delegated Regulation 2024/1502, and falls within the Art. 31(8)(iv) single-Member-State exclusion. Oversight runs through the client contract and Italian authorities' inspection powers (Art. 8, Legislative Decree 23/2025). Amazon Web Services EMEA SARL, which runs Trailgun's infrastructure and AI models, is a designated CTPP (list of 18 November 2025).
- **Criticality.** The client assesses whether Trailgun supports a critical or important function. Section 2 gives use-case guidance: data-tape remediation and public-guarantee enforcement are the likeliest to qualify; drafting and file analysis usually are not.

EN.2 Contract coverage

- **DORA Annex** (document 18, signable Word file) covering every item of Art. 30(2)(a)-(i) and 30(3)(a)-(f), Art. 28(7)-(8), Art. 29 and Delegated Regulation 2025/532. Section B (critical or important functions) is activated by the client's declaration. Roadmap milestones are binding by reference.
- **Register of information** sheet (document 16) pre-filled per Implementing Regulation 2024/2956 (B_05.01 with Trailgun's LEI, B_02.02, B_05.02 with ranks, B_07.01 inputs).
- **Subcontracting.** 60 days' notice of material changes for critical or important functions (30 days otherwise). A change takes effect only after express approval or expiry without objection, never while an objection is pending; termination without penalty if unresolved within 30 days. Sub-processors published at https://trailgun.ai/subprocessors.
- **Audit.** Unlimited access, inspection and audit rights for critical or important functions and for authorities, including Banca d'Italia; otherwise one audit per year on 30 days' notice; pooled audits accepted; questionnaires answered within 15 business days.

EN.3 Numbers that apply to every document of the pack

- **ICT incidents:** initial notice within 2 hours of awareness; updates at least every 24 hours; intermediate report within 48 hours; final report within 20 days of closure. Significant cyber threats within 24 hours. Personal data breaches within 24 hours. Assistance at no extra cost.
- **Availability:** 99.5% monthly (24/7) and 99.8% in business hours, measured every minute by an external probe. Service credits from 5% to 30%. Higher levels with the new platform (R12, R14).
- **Recovery:** RPO 24 hours; RTO 8 hours in region, measured in the quarterly restore drill; maximum tolerable downtime 5 business days; encrypted copies in Ireland. Shorter RPO and regional RTO: R01, R03, R14.
- **Exit:** transition of up to 12 months for DORA clients (30 days standard); full export within 10 business days with a return certificate; 30 days read-only access; deletion within a further 30 days with a deletion certificate; backups gone within 14 more. Source-code escrow: R09.
- **Testing:** restore drill on every CI check and quarterly on the real snapshot; yearly continuity test; participation in the client's TLPT, including pooled testing. Independent penetration test: R06.

EN.4 Current state

- **In place:** AWS Frankfurt in a dedicated account, infrastructure as code; Claude models and embeddings on Amazon Bedrock in EU regions; encrypted disks, TLS with HSTS; mandatory TOTP MFA for all users; tenant isolation through a single tested visibility check; no SSH, temporary admin credentials with MFA; CloudTrail, GuardDuty, 24/7 alerts; HTTP access and application logs 90 days; daily snapshots with encrypted copies in Ireland; protected branches and mandatory checks including secret scanning; continuity plan; incident procedure and register; supplier register; complete deletion at exit.
- **Roadmap (document 12):** independent penetration test, ISO/IEC 27001 certification, source-code escrow, multi-AZ platform, dedicated security officer.
- **Contacts:** security@trailgun.ai (24/7 for priority 1) and privacy@trailgun.ai; legal representative Franco Puppo, CEO.

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

Con questo documento: 18 Allegato DORA al contratto (Word), 16 Scheda per il Registro delle informazioni e 17 Mappa DORA (Excel), 55 SLA, 56 Piano di uscita, 57 Escrow, 51 Modelli di notifica, 12 Percorso. L'indice completo del pacchetto di conformità è nel Trust Center (documento 00).