Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO 11

VERSIONE 2.0 · DICEMBRE 2026

Continuità operativa, ripristino e incidenti

Il piano di continuità operativa e di ripristino di Trailgun, adottato e provato: analisi d'impatto, obiettivi, ruoli, otto scenari con le loro risposte e il piano di comunicazione. Con la sintesi della gestione degli incidenti TIC, delle violazioni dei dati personali e del programma di prove, i cui passi operativi stanno nelle procedure 25, 26, 30 e 31.

RPO	RTO	NOTIFICA INCIDENTI	VIOLAZIONI DATI
24 ore	8 ore	2 ore	24 ore

QUADRO D'INSIEME

Tempi scritti prima, misurati dopo

Questo documento dice come Trailgun tiene in piedi il servizio, come lo rimette in piedi e come informa i Clienti. I tempi sono quelli del contratto, e l'RTO è misurato: la prova di ripristino sullo snapshot reale si svolge ogni trimestre, e la prova automatica a ogni verifica del codice.

24h
RPO: snapshot giornaliero in Germania e in Irlanda, più una copia prima di ogni rilascio

8h
RTO nella stessa regione, misurato con la prova trimestrale di ripristino

2h
notifica iniziale di un incidente TIC al Cliente, 24/7

24h
avviso di una violazione dei dati personali al Titolare

A — **Piano di continuità operativa e di ripristino** — ARTT. 11-12, 14 DORA
Analisi d'impatto, obiettivi, ruoli, attivazione, otto scenari, procedure di ripristino, piano di comunicazione.

B — **Gestione degli incidenti TIC** — ARTT. 17-19 DORA
Classificazione a tre livelli, tempi di notifica, modelli e registro. Procedura completa: documento 25.

C — **Violazioni dei dati personali** — ARTT. 33-34 GDPR
Avviso al Titolare, assistenza, registro. Procedura completa: documento 26.

D — **Programma di prove** — ARTT. 24-25 DORA
Prova automatica, prova trimestrale, esercitazioni, test dei Clienti. Programma completo: documento 31.

Stato del documento. Versione 2.0, stato al 01/12/2026. Titolare: il Responsabile della sicurezza (Franco Puppo, CEO). Piano adottato dall'organo amministrativo con delibera del [data]. Revisione e prova ogni anno, dopo ogni incidente grave e dopo ogni cambiamento rilevante dell'architettura. Le tappe successive (copie più frequenti, ripristino regionale provato, piattaforma su più zone) sono nel documento 12, Percorso di certificazione e piattaforma.

SUMMARY IN ENGLISH

Business continuity, recovery and incident handling

This document is Trailgun's adopted business continuity and disaster recovery plan, with a summary of its ICT incident management, personal data breach handling and testing programme. The operational steps are in procedures 25 (incident response), 26 (personal data breaches), 30 (backup and restore) and 31 (disaster recovery testing). It is written for clients subject to DORA (Regulation (EU) 2022/2554), including Italian art. 106 intermediaries, and for their DPOs.

Architecture relevant to continuity

Production runs on one EC2 instance in eu-central-1 (Frankfurt), with its databases and files on one encrypted EBS volume. The whole volume is snapshotted daily at 02:00 UTC and before every production release; snapshots are kept for 14 days and copied, encrypted, to eu-west-1 (Ireland). The infrastructure is defined as code (AWS CDK) and can be rebuilt. An external probe checks the service every minute and alarms are watched 24/7. The multi-AZ platform is milestone R12 of document 12.

Recovery objectives

OBJECTIVE	COMMITMENT	HOW IT IS PROVEN
RPO	24 hours	age of the snapshot in every restore drill
RTO, same region	8 hours	measured in the quarterly restore drill
Maximum tolerable disruption	5 business days	business impact analysis (part A.1)
Loss of the Frankfurt region	copies in Ireland; tested regional procedure and RTO: milestones R03 and R10	

Every CI verification runs an automated restore drill; every quarter the latest production snapshot is restored on an isolated throw-away instance, checked for integrity and timed, and the signed record is available to clients (always to DORA clients).

Incident notification to clients

STEP	TRAILGUN COMMITS TO	SO THAT THE CLIENT CAN MEET (REG. (EU) 2025/301)
Initial notice	2 h from awareness	4 h from classification as major, 24 h from awareness
Updates	every 24 h and on any material change	–
Intermediate report	48 h from the initial notice	72 h from the client's initial notification
Final report	20 days from closure	1 month from the last intermediate report
Personal data breach	24 h to the controller	72 h to the supervisory authority (art. 33 GDPR)

Incidents are classified in three levels (major, significant, minor) on the criteria of Delegated Regulation (EU) 2024/1772; the classification as «major» under DORA remains the client's. Assistance in ICT incidents is provided at no additional cost (art. 30(2)(f) DORA).

PARTE A · PIANO DI CONTINUITÀ OPERATIVA E DI RIPRISTINO

Tenere in piedi il servizio e rimetterlo in piedi

Il piano copre la piattaforma Trailgun di production e i processi che servono a erogarla. Gli ambienti development e staging si ripristinano con le stesse procedure, senza tempi garantiti.

TITOLARE	APPROVAZIONE	VERSIONE	REVISIONE
Responsabile della sicurezza	Organo amministrativo, delibera del [data]	2.0 · stato al 01/12/2026	annuale, dopo ogni prova e ogni incidente grave

RIFERIMENTI

DORA artt. 11, 12 e 14; art. 16, par. 1, lett. f)-g) per gli intermediari 106; Reg. del. (UE) 2024/1774 art. 25 e artt. 39-40; art. 30, par. 3, lett. c), DORA; GDPR art. 32, par. 1, lett. b)-c); ISO/IEC 27001:2022 controlli 5.29, 5.30, 8.13, 8.14; ISO 22301:2019 come guida.

A.1 Che cosa conta per il Cliente

Per un avvocato o un servicer, l'interruzione di Trailgun pesa se impedisce di preparare in tempo un atto con una scadenza (un ricorso, una domanda di ammissione al passivo, una richiesta di escussione) o di rispondere a una richiesta della vigilanza. Il periodo massimo tollerabile di interruzione assunto dal piano è di **5 giorni lavorativi**: oltre, le scadenze dei Clienti sono a rischio. In ogni momento il deposito resta possibile all'avvocato con gli elaborati già scaricati, e il lavoro può proseguire a mano: Trailgun prepara, il professionista decide e deposita.

A.2 Analisi d'impatto sui processi

I processi in ordine di ripristino. Tutti condividono l'istanza e il disco dati di production, quindi l'RTO del servizio vale per tutti; l'ordine dice che cosa si verifica e si riapre per primo.

#	PROCESSO	DIPENDE DA	IMPATTO DELL'INTERRUZIONE	RIPIEGO DEL CLIENTE
1	**Accesso e consultazione** delle pratiche, download degli elaborati	istanza, disco dati, Cognito, Caddy, DNS	il Cliente non vede né scarica il lavoro fatto	elaborati già scaricati
2	**Lavorazioni**: estrazione, riconoscimento del testo, analisi, redazione, domande al faldone	come 1, più Amazon Bedrock (modelli), Textract, Transcribe	le pratiche non avanzano; quelle in corso si interrompono	lavoro manuale; ripresa senza costi
3	**Ingresso** da API, caselle email e lotti	come 2, più il fornitore di posta in entrata	le richieste restano in attesa; le email si ricevono quando il servizio torna	caricamento dal modulo al ripristino
4	**Comunicazioni** ai clienti dello studio e trattative	come 1, più il fornitore di posta	richieste e risposte ritardate	email dirette dello studio
5	**Ricerca fonti** e verifica giurisprudenziale	come 2, più One LEGALE	atti senza verifica delle fonti	ricerca dell'avvocato sulle banche dati
6	**Firma e visure**	Openapi e Namirial	firma e visure non disponibili in app	strumenti di firma dello studio
7	**Assistenza** in app	come 2	niente chat di supporto	info@ e, per la priorità 1, telefono di reperibilità
8	**Fatturazione e Amministrazione**	come 1, più il fornitore dei pagamenti	nessun impatto sulle pratiche	ripresa al ripristino

A.3 L'architettura, vista dalla continuità

- Production gira su **un'istanza EC2** a Francoforte. Database e file stanno su **un disco EBS cifrato** nella stessa zona di disponibilità: un guasto dell'istanza, del disco o della zona si risolve con il ripristino entro l'RTO di 8 ore. La piattaforma su più zone è la tappa R12 del Percorso (documento 12).
- L'infrastruttura è descritta come codice (AWS CDK) ed è ricostruibile; il disco dati è conservato anche se lo stack viene rimosso; le immagini dell'app sono nel registro ECR (ultime 15), i segreti in SSM Parameter Store.
- Copie: snapshot giornaliero alle 02:00 UTC conservato 14 giorni e copiato cifrato in Irlanda, conservato 14 giorni; snapshot prima di ogni rilascio, conservato 14 giorni; copia del database prima di ogni migrazione (documento 30).
- Monitoraggio: sonda esterna ogni minuto e allarmi 24/7 su salute, disco, CPU, memoria, errori 5xx e scadenza dei certificati; GuardDuty e CloudTrail in tutte le regioni.
- Le lavorazioni vivono nel processo: un riavvio interrompe quelle avviate dal modulo, che si riavviano senza costi; quelle in coda (API, caselle, lotti) ripartono da sole.
- Stack, immagini, segreti e pool degli utenti stanno a Francoforte; le copie dei dati anche in Irlanda.

A.4 Obiettivi di ripristino

OBIETTIVO	IMPEGNO	COME SI MISURA
RPO (dati che si possono perdere)	24 ore	età della copia usata; nei giorni di rilascio la copia pre-rilascio lo riduce a pochi minuti
RTO nella stessa regione	8 ore di calendario dalla dichiarazione dell'incidente	prova trimestrale sullo snapshot reale; prima prova del [data], RTO misurato [hh:mm]
Periodo massimo di interruzione	5 giorni lavorativi	analisi d'impatto (A.1)
Disponibilità	99,5 % mensile 24/7; 99,8 % nei giorni lavorativi 08:00-20:00	sonda esterna ogni minuto (documento 55)
Perdita della regione	copie in Irlanda; procedura regionale provata e relativo RTO: tappe R03 e R10 del Percorso (documento 12). Gli obiettivi successivi di RPO e RTO: tappe R01 e R14.	

A.5 Ruoli

I ruoli del piano sono distinti, ciascuno con un titolare e un sostituto, perché il sostituto sappia che cosa fare anche senza istruzioni. L'elenco dei contatti (referenti dei Clienti, sostituti, supporto AWS e dei fornitori, consulenti) si tiene anche fuori dalla piattaforma, in copia cifrata accessibile al sostituto, e si verifica a ogni esercitazione annuale.

RUOLO	COMPITI	TITOLARE	SOSTITUTO
Responsabile del piano	Dichiara l'attivazione del piano e la sua chiusura; decide il ripristino in un'altra regione; riferisce all'organo amministrativo	CEO	[nome]
Gestore dell'incidente	Guida la risposta tecnica, tiene il registro con gli orari, sceglie le procedure	Responsabile della sicurezza	[nome]
Comunicazione	Notifiche ai Clienti nei tempi della parte B, aggiornamenti, messaggi agli utenti	Responsabile della sicurezza	[nome]
Protezione dei dati	Valuta se c'è violazione dei dati personali, guida la parte C	DPO [...]	privacy@trailgun.ai
Supporto esterno	Assistenza AWS; analisi forense; consulente legale	[contratti]	–

A.6 Attivazione

A.6.1 Il piano si attiva quando un incidente rende o può rendere indisponibile il servizio per un Cliente oltre 2 ore, quando sono a rischio i dati (perdita, corruzione, cifratura malevola) o quando cade un fornitore essenziale. Chi rileva l'evento (allarme, Cliente, fornitore, personale) avvisa il Gestore dell'incidente al numero di reperibilità e a security@trailgun.ai.

A.6.2 Il Responsabile del piano dichiara l'attivazione e annota l'ora: da lì decorre l'RTO. Contemporaneamente parte la procedura degli incidenti (documento 25) con la notifica iniziale ai Clienti entro 2 ore.

A.6.3 Prima di ripristinare si preservano le evidenze: snapshot del disco nello stato in cui si trova, copia dei log disponibili.

A.6.4 Se dopo 4 ore la causa non è risolta nella stessa zona, si avvia il ripristino in un'altra zona di Francoforte; se la regione intera non è disponibile, il Responsabile del piano decide fra l'attesa e la ricostruzione in Irlanda (documento 30, caso 4).

A.6.5 Il piano si chiude quando il servizio è ripristinato e verificato, i Clienti sono informati e il riesame post-incidente è fissato.

A.7 · SCENARI

Otto scenari, che cosa succede e che cosa si fa

Per ogni scenario: effetto sul servizio, come si rileva, la risposta e la procedura, gli obiettivi che valgono, i presidi in essere.

S1 Perdita della regione di Francoforte

RARO · IMPATTO MOLTO ALTO

EFFETTO	Istanza, disco, snapshot locali, immagini, segreti, pool degli utenti, log non disponibili. Servizio fermo per tutti i Clienti.
RILEVAZIONE	Sonda esterna e allarmi 24/7; pagina di stato di AWS; segnalazioni dei Clienti.
RISPOSTA	Notifica ai Clienti entro 2 ore. Se AWS non prevede un ripristino rapido, ricostruzione in Irlanda dalle copie (documento 30, caso 4): nuovo pool e nuovo invito degli utenti, che registrano di nuovo l'app di autenticazione. Il lavoro dopo l'ultima copia in Irlanda si rifà.
OBIETTIVI	RPO: l'ultima copia in Irlanda (al più 24 ore). RTO regionale: tappe R03 e R10 del Percorso (documento 12).
PRESIDI	COPIE CIFRATE IN IRLANDA · INFRASTRUTTURA COME CODICE · PROCEDURA SCRITTA (DOCUMENTO 30)

S2 Interruzione di un servizio AWS

POSSIBILE · IMPATTO ALTO

EFFETTO	Guasto dell'istanza o del disco (EC2, EBS), della zona; oppure di un servizio regionale: Cognito (niente login), Textract o Transcribe (niente riconoscimento del testo o trascrizione), SSM (niente amministrazione), Route 53.
RILEVAZIONE	Sonda esterna ogni minuto e allarmi 24/7, errori nei log, AWS Health.
RISPOSTA	Istanza, disco o zona: documento 30, caso 3, con l'istanza ricreata nella stessa zona o in un'altra zona di Francoforte. Cognito: si attende AWS e si informano i Clienti. Textract o Transcribe: i documenti da leggere e gli audio da trascrivere si elaborano al ritorno del servizio, e la lavorazione si riavvia senza costi; per gli studi che hanno acceso la riserva DocuPipe, la riserva subentra per i singoli file.
OBIETTIVI	RTO 8 ore, RPO dell'ultimo snapshot.
PRESIDI	SONDA E ALLARMI 24/7 · SNAPSHOT E INFRASTRUTTURA COME CODICE · PROVA TRIMESTRALE DI RIPRISTINO

S3 Indisponibilità dei modelli

POSSIBILE · IMPATTO ALTO

EFFETTO	Gli agenti non rispondono: le lavorazioni non procedono, l'assistente e la chat di supporto tacciono. Accesso, consultazione e download funzionano.
RILEVAZIONE	Errori delle chiamate ai modelli nei log; allarme sugli errori.
RISPOSTA	I modelli girano su Amazon Bedrock nella regione di Francoforte. Per un guasto di Bedrock si informano i Clienti, si sospendono gli avvii e si riprendono le lavorazioni al ritorno senza costi. **Nessun ripiego verso un fornitore o una regione fuori dall'UE**: il codice rifiuta le regioni non UE.
OBIETTIVI	Dipende da AWS; il periodo massimo di 5 giorni lavorativi vale anche qui.
PRESIDI	BEDROCK A FRANCOFORTE · RIPRESA SENZA COSTI

S4 Persona chiave non disponibile

POSSIBILE · IMPATTO MOLTO ALTO

EFFETTO	Il servizio continua a funzionare, ma rilasci, ripristini e risposte agli incidenti richiedono chi ha l'accesso tecnico.
RILEVAZIONE	Assenza non pianificata oltre un giorno lavorativo, o mancata risposta alla reperibilità entro un'ora.
RISPOSTA	Il sostituto [nome] apre l'accesso di emergenza custodito presso [luogo o depositario] (credenziali dell'account AWS e dei fornitori, dispositivo MFA), segue le procedure di questo documento e dei documenti 25 e 30, informa i Clienti se un impegno è a rischio e, se serve, incarica il fornitore tecnico [nome]. L'uso dell'accesso di emergenza si registra.
OBIETTIVI	Gli stessi del servizio: lo scenario non sposta disponibilità, RTO e RPO.
PRESIDI	SOSTITUTO DESIGNATO · ACCESSO DI EMERGENZA CUSTODITO · PROCEDURE SCRITTE · deposito del codice e responsabile della sicurezza dedicato: tappe R09 e R13 (documento 12)

S5 Ransomware o compromissione

RARO · IMPATTO MOLTO ALTO

EFFETTO	Dati cifrati o cancellati da un attaccante, credenziali rubate, possibile esfiltrazione. È insieme un incidente TIC e, probabilmente, una violazione dei dati personali.
RILEVAZIONE	GuardDuty e CloudTrail, allarmi, anomalie nei dati, segnalazioni.
RISPOSTA	Documento 25: revoca delle credenziali (RB-05), isolamento e ricostruzione pulita (RB-08), ripristino da una copia anteriore alla compromissione. Documento 26 per i dati personali. Nessun pagamento di riscatto.
OBIETTIVI	RTO 8 ore se esiste una copia pulita; RPO fino all'ultima copia pulita.
PRESIDI	COPIE IN DUE REGIONI · GUARDDUTY E CLOUDTRAIL · CREDENZIALI TEMPORANEE · copie protette dalla cancellazione: tappa R11 (documento 12)

S6 Corruzione dei dati

POSSIBILE · IMPATTO ALTO

EFFETTO	Database danneggiato, migrazione errata, cancellazione per errore, file mancanti. Il servizio può restare su ma con dati sbagliati: è l'integrità, non la disponibilità.
RILEVAZIONE	Errori dell'app, controllo d'integrità del database lanciato a mano, segnalazioni dei Clienti, stato delle migrazioni nella pagina «Sistema».
RISPOSTA	Si fermano le scritture (manutenzione urgente), si fotografa il disco, si individua l'istante buono: copia del database prima della migrazione, snapshot prima del rilascio, snapshot giornaliero. Documento 30, casi 1 e 2. Si dice ai Clienti quali pratiche ricontrollare o rifare.
OBIETTIVI	RPO dell'ultima copia buona; RTO 8 ore.
PRESIDI	MIGRAZIONI SOLO IN AVANTI E COPIA PRIMA DI OGNUNA · PROVA AUTOMATICA DI RIPRISTINO A OGNI VERIFICA

S7 Guasto di un fornitore

PROBABILE · IMPATTO MEDIO

EFFETTO	Posta dell'app: niente email in uscita né risposte in entrata. One LEGALE: niente ricerca fonti (un solo account). Openapi: niente firma e visure. GitHub: niente rilasci dall'integrazione continua. Let's Encrypt: certificati non rinnovati (validità residua fino a 90 giorni). Google Workspace: posta delle persone.
RILEVAZIONE	Errori nei log, pagine di stato dei fornitori, allarme sulla scadenza dei certificati.
RISPOSTA	RB-07 (sotto): funzione degradata dichiarata ai Clienti, ripiego della tabella A.2, ripresa al ritorno. Un fornitore che cessa si sostituisce con la comunicazione urgente entro 72 ore (documento 29). Un rilascio urgente senza GitHub si fa con lo script di rilascio manuale (documento 20).
OBIETTIVI	Il servizio principale resta disponibile; la funzione accessoria torna con il fornitore.
PRESIDI	FUNZIONI ACCESSORIE SEPARATE · REGISTRO DEI FORNITORI CON PIANI DI USCITA

S8 Rilascio difettoso o risorsa esaurita

PROBABILE · IMPATTO MEDIO

EFFETTO	Una versione nuova rompe una funzione, oppure il disco di sistema si riempie e il servizio non riparte (è successo il 21/10/2026, incidente registrato senza perdita né esposizione di dati).
RILEVAZIONE	Verifica di `/api/health` a fine rilascio, segnalazioni, allarmi su disco e memoria.
RISPOSTA	Ritorno alla versione precedente (documento 20): le migrazioni sono compatibili con l'immagine precedente, quindi i dati non si toccano. Disco pieno: pulizia delle immagini locali, che restano in ECR, ed eventuale ampliamento del volume; la pulizia avviene comunque a ogni rilascio.
OBIETTIVI	Entro la manutenzione urgente; RTO 8 ore al più.
PRESIDI	VERIFICA OBBLIGATORIA PRIMA DI OGNI RILASCIO · SNAPSHOT PRIMA DEL RILASCIO · ALLARMI SU DISCO E MEMORIA

A.8 · PROCEDURE DI RIPRISTINO

Dove sono scritti i passi

Ogni procedura è scritta e la si segue annotando ogni passo, con l'ora, nel registro dell'incidente. I casi di ripristino del documento 30 sono provati ogni trimestre (documento 31).

CODICE	PROCEDURA	DOVE
RB-01	Ripristino del disco dati nella stessa regione	documento 30, casi 2 e 3
RB-02	Ricostruzione dell'istanza	documento 30, caso 3
RB-03	Ripristino in Irlanda	documento 30, caso 4; procedura regionale provata: tappe R03 e R10
RB-04	Ritorno alla versione precedente	documento 20, paragrafo 9
RB-05	Credenziali compromesse	documento 25, paragrafo 8; documento 23, paragrafo 5
RB-06	Dati corrotti o cancellati per errore	documento 30, casi 1 e 2
RB-07	Funzione degradata per un fornitore	qui sotto
RB-08	Isolamento e ricostruzione pulita	documento 25, paragrafo 9

RB-07 Funzione degradata per un fornitore

1. Confermare il guasto sulla pagina di stato del fornitore o con il suo supporto; aprire una segnalazione presso di lui.
2. Informare i Clienti della funzione non disponibile e del ripiego; sospendere gli avvii che dipendono da quel fornitore.
3. Al ritorno, riprendere le lavorazioni sospese senza costi e verificare che le email ricevute nel frattempo siano arrivate.
4. Se il guasto supera la tolleranza della funzione, attivare il piano di uscita del fornitore nel registro dei subfornitori (documento 15) con le regole del documento 29.

A.9 · PIANO DI COMUNICAZIONE

Chi informiamo, quando e come

Il canale non dipende dalla piattaforma: se la piattaforma è ferma, si scrive dalla posta aziendale su Google Workspace e si telefona.

DESTINATARIO	QUANDO	CANALE	CHE COSA
Referenti sicurezza del Cliente (Modulo d'ordine)	entro 2 ore; aggiornamenti ogni 24 ore e a ogni novità; per le priorità 1 ogni 2 ore fino al ripristino	email da security@trailgun.ai; telefono per le priorità 1	modelli del documento 51
DPO del Titolare	entro 24 ore se ci sono dati personali coinvolti	email da privacy@trailgun.ai	avviso del documento 26
Amministratori degli studi	all'inizio e alla fine di un'interruzione o manutenzione urgente	email	che cosa non funziona, ripiego, prossimo aggiornamento
Utenti	a servizio ripristinato	email	che cosa rifare (pratiche dopo l'ultima copia)
Fornitori	subito, se coinvolti	canale di supporto del fornitore	segnalazione e richiesta di informazioni
Autorità	tramite il Cliente; su richiesta, direttamente	secondo l'autorità	cooperazione piena (art. 30, par. 2, lett. g), DORA)
Organo amministrativo	all'attivazione del piano	telefono, email	stato, decisioni da prendere

A.10 Messaggio tipo per un'interruzione

Oggetto: [Trailgun] Interruzione del servizio · codice INC-[aaaa-nnn] · aggiornamento [n]. Dalle [ora] del [data] la piattaforma [non è raggiungibile / non avvia nuove lavorazioni]. Causa accertata o ipotizzata: [...]. I vostri dati: [nessuna evidenza di perdita o accesso / in accertamento]. Che cosa fare nel frattempo: [ripiego]. Ripristino previsto: [ora]. Prossimo aggiornamento entro le [ora]. Referente: [nome], security@trailgun.ai, [+39 ...].

PARTE B · GESTIONE DEGLI INCIDENTI TIC

Rilevare, classificare, contenere, informare, imparare

La sintesi della procedura che Trailgun segue per ogni incidente che tocca o può toccare il servizio o i dati dei Clienti. Il testo completo, con ruoli, passi, matrice di gravità e contenimento, è il documento 25.

B.1 Le fasi

1. **Registrazione** nel registro degli incidenti, con un codice INC-*aaaa-nnn*; il registro raccoglie tutti gli incidenti e le minacce significative (art. 17, par. 2, DORA).
2. **Classificazione** entro la prima ora, e di nuovo a ogni informazione nuova (B.2).
3. **Contenimento**, preservando prima le evidenze.
4. **Notifica** ai Clienti interessati entro 2 ore (B.3), anche con informazioni parziali.
5. **Eliminazione della causa e ripristino** con le procedure della parte A.
6. **Chiusura**, quando il servizio è ripristinato e verificato e la causa è rimossa o mitigata.
7. **Riesame** post-incidente (art. 13, par. 2, DORA), con azioni, titolari e date, e aggiornamento del registro dei rischi.

B.2 Classificazione

Tre livelli, **grave**, **significativo** e **minore**, sui criteri del Reg. del. (UE) 2024/1772: servizi critici colpiti, perdite di dati, durata e tempo di inattività, clienti colpiti, diffusione geografica, impatto economico e reputazionale, ricorrenza. Per Trailgun basta un criterio per il livello più alto: un accesso non autorizzato ai dati di un Cliente, qualsiasi dato di un fascicolo penale, una perdita oltre l'RPO, un'indisponibilità oltre 2 ore o un incidente aperto oltre 24 ore sono gravi. La qualifica di «incidente grave» ai sensi dell'art. 19 DORA la decide il Cliente sui propri criteri: per l'art. 8 del regolamento, con servizi critici colpiti, serve un accesso malevolo riuscito che può portare a perdite di dati oppure il superamento di due o più soglie. La classificazione di Trailgun scatta prima, perché il Cliente abbia i dati in tempo.

B.3 Tempi di notifica al Cliente

PASSO	TRAILGUN	IL CLIENTE DORA (REG. DEL. (UE) 2025/301, ART. 5)
Notifica iniziale	entro 2 ore dalla conoscenza, per email e telefono	4 ore dalla classificazione come grave, 24 ore dalla conoscenza
Aggiornamenti	almeno ogni 24 ore e a ogni cambiamento rilevante; per le priorità 1 ogni 2 ore	–
Relazione intermedia	entro 48 ore dalla notifica iniziale	72 ore dalla notifica iniziale
Relazione finale	entro 20 giorni dalla chiusura	un mese dall'ultima relazione intermedia
Minacce significative	entro 24 ore	notifica volontaria (art. 19, par. 2, DORA)

B.4 Modelli, registro, assistenza

B.4.1 I quattro modelli (notifica iniziale, relazione intermedia, relazione finale, minaccia significativa) sono il documento 51, in Word. I campi seguono i dati che il Cliente deve inserire nei moduli del Reg. es. (UE) 2025/302, compresa l'origine dell'incidente presso un fornitore terzo.

B.4.2 Il registro degli incidenti è tenuto da Trailgun e il Cliente ne riceve l'estratto delle voci che lo riguardano, su richiesta e in audit. Vi è registrato l'incidente operativo di disponibilità del 21/10/2026 (scenario S8), senza perdita né esposizione di dati.

B.4.3 L'assistenza al Cliente nella gestione di un incidente legato al servizio è senza costi aggiuntivi (art. 30, par. 2, lett. f), DORA). Trailgun non presenta segnalazioni alle autorità per conto del Cliente salvo accordo scritto; anche in quel caso il Cliente ne resta pienamente responsabile (art. 19, par. 5, DORA).

PARTE C · VIOLAZIONI DEI DATI PERSONALI

Avvisare il Titolare entro 24 ore

Per i dati delle pratiche il Titolare è lo studio, la banca o il servicer, e Trailgun è responsabile del trattamento. Il testo completo è il documento 26; le richieste degli interessati seguono il documento 27.

C.1 Ogni incidente si esamina anche come possibile violazione dei dati personali. Trailgun avvisa il Titolare **entro 24 ore** dalla conoscenza, senza ingiustificato ritardo, con i contenuti dell'art. 33, par. 3, GDPR, e completa le informazioni per fasi; per il Titolare soggetto a DORA vale anche la notifica iniziale di 2 ore della parte B.

C.2 Trailgun assiste il Titolare nella notifica al Garante entro 72 ore e nella comunicazione agli interessati, senza comunicare con loro o con il Garante per suo conto senza istruzione. Una violazione che tocca un fascicolo penale si presume ad alto rischio.

C.3 Il registro delle violazioni è tenuto da Trailgun; l'estratto va al Titolare su richiesta.

C.4 Per i dati degli account, dei contatti, del sito e della fatturazione Trailgun è titolare: notifica al Garante entro 72 ore, salvo che sia improbabile un rischio per le persone, e comunica agli interessati se il rischio è elevato.

C.5 Le richieste degli interessati si inoltrano al Titolare entro 3 giorni lavorativi; le informazioni per la valutazione d'impatto del Titolare arrivano entro 10 giorni lavorativi.

PARTE D · PROGRAMMA DI PROVE

Un piano non provato è un'ipotesi

Il piano si prova a ogni verifica del codice, ogni trimestre e ogni anno. Il programma completo, con i criteri di successo e i verbali, è il documento 31; i passi di ripristino sono il documento 30.

PROVA	FREQUENZA	CHE COSA DIMOSTRA
Prova automatica di ripristino	a ogni verifica del codice	che la copia coerente del database e la copia grezza del disco si ripristinano senza differenze in schema, righe e file
Prova sullo snapshot reale in un ambiente isolato	ogni trimestre e dopo ogni cambiamento dell'infrastruttura	che l'ultimo snapshot di production si ripristina e i database sono integri; RPO e RTO reali. Prima prova del [data]: RTO misurato [hh:mm], esito [superata]
Esercitazione a tavolino	ogni anno	ruoli, decisioni, comunicazioni e una notifica completa a un Cliente DORA su uno o più scenari S1-S8; contatti raggiungibili
Test dei Clienti	secondo il Cliente	partecipazione ai test di continuità e ai test guidati dalla minaccia (art. 26 DORA), alle condizioni concordate per non mettere a rischio gli altri Clienti

D.1 Le prove non toccano production: il volume si crea dallo snapshot su un'istanza temporanea senza traffico in ingresso, dall'istanza escono solo conteggi e orari, e tutte le risorse di prova si cancellano a fine prova.

D.2 Gli esiti vanno al Cliente che li chiede e sempre ai Clienti DORA. Il Cliente DORA può partecipare all'esercitazione annuale.

D.3 Le prove delle tappe successive (ripristino regionale completo, penetration test indipendente, nuova piattaforma su più zone) sono nel documento 12, tappe R10, R06 e R12.

Trailgun

On target.

In a flash.

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

SICUREZZA E INCIDENTI, 24/7
security@trailgun.ai

REPERIBILITÀ PRIORITÀ 1
[+39 ...]

PRIVACY E DPO
privacy@trailgun.ai

Documento 11 del pacchetto di conformità Trailgun, versione 2.0, stato al 01/12/2026. Le procedure operative sono i documenti 25 (risposta agli incidenti), 26 (violazioni dei dati personali), 30 (backup e ripristino) e 31 (prova di disaster recovery); i modelli di notifica sono il documento 51; le tappe successive sono nel documento 12. Documento riservato, destinato al Cliente e alle sue autorità di vigilanza.