Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO P02

VERSIONE 2.0 · DICEMBRE 2026

Politica di gestione del rischio ICT

Il metodo con cui Trailgun individua, misura, tratta e riesamina i rischi per il servizio e per i dati dei Clienti: scale, propensione al rischio, rischio da terzi e di concentrazione. Il registro che ne risulta è il foglio 41.

CODICE	TITOLARE	REVISIONE	STATO
P02 · POL-02	Responsabile della sicurezza	Annuale · registro trimestrale	al 01/12/2026

POLITICA P02 · POL-02

Politica di gestione del rischio ICT

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

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

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

DOCUMENTI COLLEGATI

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

AMBITO

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

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

1 Scopo e ambito

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

2 Ruoli

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

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

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

3 Il processo

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

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

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

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

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

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

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

4 Inventario degli asset (sintesi)

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

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

5 Scale di misura

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

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

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

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

6 Propensione al rischio

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

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

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

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

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

7 Rischio da terzi e di concentrazione

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

8 Il registro dei rischi

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

9 Trasferimento del rischio

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

10 Evidenze e registri

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

11 Eccezioni e riferimenti normativi

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