Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO 29

VERSIONE 2.0 · DICEMBRE 2026

Procedura di valutazione dei fornitori

Come Trailgun valuta un fornitore prima di affidargli una parte del servizio o dei dati dei Clienti, come lo rivaluta ogni anno, come informa i Clienti di un cambio e come tiene il registro dei subfornitori e la pagina pubblica.

VALUTAZIONE
prima dell'ingaggio e ogni anno

PREAVVISO AI CLIENTI
30 giorni · 60 per DORA

SOSTITUZIONE URGENTE
comunicata entro 72 ore

ELENCO PUBBLICO
trailgun.ai/subprocessors

PROCEDURA 29 · PROC-29

Valutazione dei fornitori

Un fornitore che tratta dati dei Clienti o regge una parte del servizio si sceglie su criteri scritti, si contrattualizza con gli stessi obblighi che Trailgun ha verso i Clienti, si rivaluta ogni anno e si sostituisce con un piano.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
PROC-29	Responsabile della sicurezza, con il DPO	Organo amministrativo, [data della delibera]	2.0 · stato al 01/12/2026

REVISIONE	DESTINATARI
annuale	chi propone o gestisce un fornitore; funzione di esternalizzazione e DPO dei Clienti

DOCUMENTI COLLEGATI

politica P10; documento 15, Registro dei subfornitori; documento 16, Scheda per il Registro delle informazioni; documento 07, DPA; documento 08, DORA: Trailgun come fornitore di servizi TIC; documento 20, Gestione dei cambiamenti; documento 41, Registro dei rischi ICT

1 Scopo e ambito

1.1 La procedura vale per ogni fornitore che tratta dati dei Clienti, ospita o esegue una parte del servizio o ne condiziona la sicurezza: infrastruttura e modelli, riconoscimento del testo, posta, notifiche, firma e visure, banca dati giuridica, pagamenti, codice e integrazione continua.

1.2 I criteri sono i fattori degli artt. 5 e 6 del Reg. del. (UE) 2024/1773, che Trailgun adotta come modello, e gli obblighi dell'art. 28 GDPR verso i sub-responsabili.

2 Classi

CLASSE	CHE COSA VUOL DIRE	FORNITORI AL 01/12/2026
Essenziale	senza di lui il servizio non c'è	Amazon Web Services EMEA SARL: infrastruttura e conservazione in Germania con copie in Irlanda, modelli Claude su Amazon Bedrock nella regione di Francoforte (UE), Textract, Transcribe, Cognito, posta di sistema
Importante	tratta dati dei Clienti per una funzione accessoria	Resend (posta dell'app e risposte in entrata); Wolters Kluwer Italia (One LEGALE, banca dati giuridica, senza dati delle pratiche nelle ricerche); Openapi con Namirial (firma qualificata e visure); DocuPipe (riconoscimento del testo di riserva) solo per gli studi che lo accendono; le notifiche e i pagamenti come indicati nel registro 15
Di supporto	non riceve dati dei Clienti	GitHub (codice e integrazione continua), Google Workspace (posta delle persone), Let's Encrypt, registri di immagini e pacchetti

3 Criteri di valutazione

AREA	CHE COSA SI VERIFICA	EVIDENZA
Dati	quali dati riceve, di quale classe (politica P11), se dati penali o categorie particolari; minimizzazione possibile	schema dei flussi
Luogo	dove conserva e tratta i dati; sede del fornitore e della capogruppo; legge applicabile e accesso di autorità di paesi terzi	contratto, documentazione delle regioni
Sicurezza	certificazioni (ISO/IEC 27001, SOC 2 di tipo II, C5) con perimetro e scadenza; cifratura; notifica degli incidenti; autenticazione a più fattori sulle console	certificati, rapporti, pagine di sicurezza
Contratto	accordo ex art. 28 GDPR con gli stessi obblighi del DPA di Trailgun (art. 28, par. 4); conservazione dei dati e cancellazione; nessun uso dei dati per addestrare modelli; subfornitori del fornitore e loro preavviso	DPA firmato
Trasferimenti	se c'è un trasferimento fuori dallo Spazio economico europeo: decisione di adeguatezza o clausole contrattuali tipo (Decisione (UE) 2021/914, modulo 3) e valutazione d'impatto del trasferimento con le misure supplementari	clausole tipo, valutazione d'impatto

AREA	CHE COSA SI VERIFICA	EVIDENZA
DORA	per i servizi che un Cliente usa per una funzione essenziale o importante: diritti di accesso, ispezione e audit riconosciuti lungo la catena, cooperazione con le autorità, continuità, piani di emergenza (Reg. del. (UE) 2025/532, art. 4)	clausole, attestazioni
Solidità e condotta	reputazione, risorse, controlli; condotta etica e responsabile; sanzioni	fonti pubbliche, bilanci
Sostituibilità e uscita	alternative, dati e configurazioni da trasferire, tempi; concentrazione su uno stesso fornitore	piano di uscita nel registro

4 Prima dell'ingaggio

1 **Proposta.** Chi propone il fornitore descrive il servizio, i dati, la classe proposta e le alternative considerate.

2 **Valutazione** del Responsabile della sicurezza e del DPO sui criteri della tabella 3, con le evidenze raccolte; la valutazione d'impatto del trasferimento quando serve.

3 **Contratto** con le clausole della tabella 3, prima che il fornitore riceva qualsiasi dato dei Clienti.

4 **Rischio**: rischi residui e concentrazione nel registro dei rischi ICT (documento 41).

5 **Preavviso ai Clienti** se il fornitore tratta dati dei Clienti (paragrafo 6). Il fornitore entra in servizio solo dopo il preavviso, e per i Clienti DORA con funzioni essenziali o importanti solo senza opposizioni pendenti.

6 **Registro**: il fornitore entra nel registro dei subfornitori (documento 15) e nella pagina pubblica; l'ingaggio è un cambiamento significativo (documento 20).

5 Ogni anno e dopo un evento

5.1 Ogni fornitore essenziale e importante si rivaluta ogni anno sugli stessi criteri: certificazioni in scadenza, cambi di luogo o di subfornitori, incidenti, qualità del servizio, aggiornamento del piano di uscita. L'esito, con la data, va nel registro 15.

5.2 Si rivaluta subito dopo un incidente rilevante presso il fornitore, un cambio delle sue condizioni sui dati, una sua acquisizione, una sanzione.

5.3 Il registro fornisce al Cliente i dati della catena di fornitura che gli servono per il proprio registro delle informazioni (Reg. es. (UE) 2024/2956, modelli B_05.01 e B_05.02), raccolti nella scheda del documento 16.

6 Cambio di un subfornitore e informativa ai Clienti

6.1 L'aggiunta o la sostituzione di un subfornitore che tratta dati dei Clienti si comunica per email all'amministratore e al DPO del Cliente almeno **30 giorni** prima, con identità, attività, luogo e garanzie.

6.2 Per i Clienti DORA che usano Trailgun per una funzione essenziale o importante il preavviso è di **60 giorni**; il cambiamento non si attua prima della scadenza né finché un'opposizione è pendente (Reg. del. (UE) 2025/532, art. 5).

6.3 Il Cliente può opporsi entro il periodo di preavviso; se l'opposizione non si risolve in 30 giorni, può recedere senza penali, con il rimborso della quota pagata e non goduta.

6.4 Una sostituzione urgente, solo per sicurezza o per cessazione del fornitore, si comunica entro 72 ore; il diritto di opposizione resta.

6.5 L'elenco dei subfornitori è allegato al DPA e pubblicato su https://trailgun.ai/subprocessors, aggiornato a ogni cambio.

7 Uscita e concentrazione

Per ogni fornitore essenziale e importante il registro tiene un piano di uscita: alternativa individuata, dati e configurazioni da trasferire, tempi. L'infrastruttura descritta come codice e i formati aperti dei dati riducono la dipendenza da AWS; la concentrazione su AWS, che è anche fornitore terzo critico designato dalle autorità europee di vigilanza, è un rischio accettato e monitorato nel registro dei rischi. Nessun ripiego verso un fornitore di modelli fuori dall'UE si attiva senza istruzione scritta del Cliente.

8 Evidenze e riferimenti

8.1 Evidenze: registro dei subfornitori (documento 15) con data dell'ultima valutazione; fascicolo di ogni fornitore (valutazione, DPA, clausole tipo e valutazioni d'impatto dei trasferimenti, certificati); preavvisi inviati ai Clienti con la data; storico della pagina pubblica.

8.2 Riferimenti: DORA, artt. 28 e 29 e art. 30; Reg. del. (UE) 2024/1773, artt. 5 e 6; Reg. del. (UE) 2025/532, artt. 3-5; Reg. es. (UE) 2024/2956; GDPR, art. 28, par. 2 e 4, e artt. 44-46; Raccomandazioni EDPB 01/2020 sulle misure supplementari; ISO/IEC 27001:2022, controlli 5.19-5.23.

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

Procedura 29 del pacchetto di conformità Trailgun, versione 2.0, stato al 01/12/2026. Attua la politica P10 (gestione dei fornitori ICT). L'elenco aggiornato dei subfornitori è il documento 15 e la pagina https://trailgun.ai/subprocessors. Documento riservato, destinato al Cliente e alle sue autorità di vigilanza.