Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO P10



VERSIONE 2.0 · DICEMBRE 2026

Politica di gestione dei fornitori ICT

Come Trailgun sceglie, contrattualizza, controlla e sostituisce i fornitori che concorrono al servizio, come ne informa i Clienti con 30 o 60 giorni di preavviso, e quali sono.

CODICE	TITOLARE	REVISIONE	STATO
P10 · POL-10	Responsabile della sicurezza, con il DPO	Annuale · registro a ogni cambio	al 01/12/2026

POLITICA P10 · POL-10

Politica di gestione dei fornitori ICT

Come Trailgun sceglie, contrattualizza, controlla e sostituisce i fornitori che concorrono al servizio, e come ne informa i Clienti.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P10 (POL-10)	Responsabile della sicurezza, con il DPO	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale; registro a ogni cambio di fornitore	uffici outsourcing, ICT risk e DPO dei Clienti	Riservato · per il Cliente

DOCUMENTI COLLEGATI

P02, P11; registro dei subfornitori (15); scheda per il registro delle informazioni (16); procedura 29 (Valutazione dei fornitori); documento 07 (DPA), Allegato 3; documento 18 (Allegato DORA al contratto)

AMBITO

Ogni fornitore che tratta dati dei Clienti, ospita o esegue una parte del servizio o ne condiziona la sicurezza: infrastruttura, modelli, riconoscimento del testo, posta, notifiche, firma, banche dati, pagamenti, codice e CI.

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
5.19-5.23	DORA artt. 28-30; Reg. del. (UE) 2025/532; GDPR artt. 28, 44-46

1 Scopo e ruoli

Il servizio di Trailgun è sicuro quanto la sua catena di fornitura. Il Responsabile della sicurezza valuta e monitora i fornitori e tiene il registro; il DPO valuta i trattamenti di dati personali e i trasferimenti; il legale rappresentante firma i contratti; l'organo amministrativo approva l'ingaggio di un fornitore essenziale.

2 Classi di fornitori

2.1 **Essenziali:** senza di loro il servizio non c'è (Amazon Web Services, che fornisce anche i modelli su Amazon Bedrock).

2.2 **Importanti:** trattano dati dei Clienti per una funzione accessoria (posta, banca dati, firma e visure, notifiche, riconoscimento del testo di riserva).

2.3 **Di supporto:** non ricevono dati dei Clienti (codice e CI, certificati, immagini e pacchetti, posta aziendale salvo la corrispondenza che i Clienti vi mandano).

3 Prima dell'ingaggio

1. **Valutazione** secondo la procedura 29: dati trattati e loro classe (P11), luogo di conservazione e di trattamento, sede del fornitore e della capogruppo, certificazioni (ISO/IEC 27001, SOC 2 di tipo II, C5), conservazione dei dati, uso dei dati per addestramento, subfornitori, solidità, sostituibilità, legge applicabile e accesso di autorità di paesi terzi, disponibilità ad audit, condotta etica. Sono i fattori degli artt. 5 e 6 del Reg. del. (UE) 2024/1773, che Trailgun adotta come modello.
2. **Trasferimenti.** Per un fornitore fuori dall'UE: base del trasferimento, clausole contrattuali tipo (Decisione di esecuzione (UE) 2021/914, modulo 3) e valutazione d'impatto del trasferimento.
3. **Decisione** registrata nel registro 15, con esito, condizioni e data della prossima valutazione. Un fornitore essenziale o importante non si ingaggia senza questa valutazione.
4. **Preavviso ai Clienti** (§ 6) prima che il fornitore riceva dati dei Clienti.

4 Contratto

Con ogni fornitore che tratta dati personali: accordo ex art. 28 GDPR con gli stessi obblighi del DPA di Trailgun verso i Clienti (art. 28, par. 4). Per i fornitori essenziali e importanti, inoltre: misure di sicurezza, notifica degli incidenti, luogo dei dati e preavviso del suo cambio, diritti di audit o rapporti indipendenti, cooperazione con le autorità, restituzione e cancellazione, uscita. Per i servizi che un Cliente DORA usa per una funzione essenziale o importante, Trailgun porta nei subcontratti quanto richiede l'art. 4 del Reg. del. (UE) 2025/532, in particolare gli stessi diritti di accesso e ispezione.

5 Monitoraggio

Il registro dei subfornitori (15) riporta per ciascuno: servizio, classe, dati, luogo, contratto e DPA, garanzie di trasferimento, certificazioni con scadenza, subfornitori rilevanti, data dell'ultima valutazione e della prossima, piano di uscita. Ogni fornitore essenziale e importante si rivaluta ogni anno e dopo un suo incidente rilevante. Il registro dà al Cliente i dati della catena di fornitura che servono al suo registro delle informazioni (Reg. es. (UE) 2024/2956, modelli B_05.01 e B_05.02; scheda 16).

6 Cambi di fornitore 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 (art. 5 del Reg. del. (UE) 2025/532).

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 cessazione del fornitore, si comunica entro 72 ore; il diritto di opposizione resta.

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

7 Uscita e concentrazione

Per ogni fornitore essenziale e importante Trailgun tiene un piano di uscita: alternativa individuata, dati e configurazioni da trasferire, tempi. L'infrastruttura come codice e i formati aperti dei dati riducono la dipendenza da AWS; la concentrazione resta un rischio accettato e monitorato (politica P02). Nessun ripiego verso un fornitore di modelli fuori dall'UE si attiva: il codice rifiuta qualsiasi regione fuori dall'UE.

8 I fornitori al 01/12/2026

Il dettaglio, con entità contrattuali, garanzie e date di valutazione, è nel registro 15.

FORNITORE E CLASSE	SERVIZIO E DATI	LUOGO	GARANZIE
Amazon Web Services EMEA SARL · essenziale	Infrastruttura, conservazione, login (Cognito), posta di Cognito (SES), Textract, Transcribe, modelli Claude e Titan su Amazon Bedrock; tutti i dati	Germania; copie in Irlanda; modelli in regione UE	DPA; opt-out dal riuso dei contenuti per i servizi di IA di AWS con policy dell'organizzazione; account intestato a Trailgun
Plus Five Five, Inc. (Resend) · importante	Email in uscita e risposte in entrata	Amazon SES in Irlanda; società USA	DPA, clausole contrattuali tipo, valutazione del trasferimento
Wolters Kluwer Italia (One LEGALE) · importante	Banca dati giuridica; riceve solo stringhe di ricerca, senza nomi, codici fiscali, importi o dati delle pratiche (regola in codice con test)	Italia	DPA
Openapi S.p.A., con Namirial · importante	Firma elettronica qualificata e visure camerali	Italia	DPA
Hoss Inc. (DocuPipe) · importante, opzionale	Riconoscimento del testo di riserva, solo per gli studi che lo accendono (spento di default); il singolo file che Textract non legge	USA	DPA, clausole contrattuali tipo, valutazione del trasferimento
Telegram, **Twilio** · per scelta dell'utente	Notifiche su Telegram, SMS e WhatsApp per chi collega quei canali; senza dati delle pratiche	secondo il fornitore	nessun dato delle pratiche nel messaggio
Stripe · per la fatturazione	Carta e addebiti dello studio; nessun dato delle pratiche	UE/USA	condizioni del fornitore
Microsoft	Login per la revisione in Word: il file va dal browser dell'avvocato al tenant del Cliente; non riceve dati da Trailgun	–	–
Google Workspace, **GitHub**, Let's Encrypt, Docker Hub, npm · di supporto	Posta delle persone; codice e CI; certificati; immagini e pacchetti; nessun dato delle pratiche	vari	MFA sulle console; 2FA obbligatoria su GitHub

9 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
DPA con i fornitori	IN ESSERE AWS, Resend, Wolters Kluwer, Openapi, DocuPipe	archivio dei contratti; registro 15
Valutazioni	IN ESSERE prima dell'ingaggio e ogni anno, con le valutazioni dei trasferimenti	procedura 29; registro 15
Elenco pubblicato	IN ESSERE allegato al DPA e pagina pubblica	https://trailgun.ai/subprocessors, a ogni cambio
Preavvisi	IN ESSERE 30 giorni, 60 per i Clienti DORA con funzioni essenziali o importanti	email all'amministratore e al DPO del Cliente

10 Eccezioni e riferimenti normativi

Eccezioni secondo P01 § 8; nessuna eccezione può ammettere un fornitore che tratti dati dei Clienti senza contratto scritto. Riferimenti: DORA artt. 28, 29 e 30; Reg. del. (UE) 2024/1773 e 2025/532; Reg. es. (UE) 2024/2956; GDPR artt. 28 e 44-46; Parere EDPB 22/2024; ISO/IEC 27001:2022 controlli 5.19-5.23.