Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO P11

VERSIONE 2.0 · DICEMBRE 2026

Politica di classificazione delle informazioni

Pubblico, interno, riservato, strettamente riservato: per ciascun livello le regole di conservazione, trasmissione, condivisione e distruzione, e la corrispondenza con la sensibilità dei dati del registro DORA.

CODICE	TITOLARE	REVISIONE	STATO
P11 · POL-11	Responsabile della sicurezza, con il DPO	Annuale	al 01/12/2026

POLITICA P11 · POL-11

Politica di classificazione e trattamento delle informazioni

Quattro livelli, con le regole di conservazione, trasmissione, condivisione e distruzione di ciascuno.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P11 (POL-11)	Responsabile della sicurezza, con il DPO	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale	tutto il personale e i collaboratori; uffici audit e DPO dei Clienti	Riservato · per il Cliente

DOCUMENTI COLLEGATI
P04, P12, P14, P16; inventario degli asset (42); registro dei trattamenti (40); scheda per il registro delle informazioni (16)

AMBITO
Tutte le informazioni che Trailgun crea, riceve o tratta, in qualsiasi forma: dati dei Clienti sulla piattaforma, documenti interni, codice, corrispondenza.

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
5.12-5.14, 8.11, 8.12	DORA art. 8; Reg. es. (UE) 2024/2956; GDPR artt. 9, 10, 32

1 Scopo e ruoli

La classificazione dice a chiunque lavori per Trailgun come trattare un'informazione senza doverlo chiedere. Il Responsabile della sicurezza assegna il livello agli asset nell'inventario (42); il DPO verifica che i dati personali, e in particolare quelli dell'art. 9 e dell'art. 10 GDPR, siano al livello giusto; ogni persona applica le regole del livello.

2 I livelli

LIVELLO	ESEMPI	REGOLE	SENSIBILITÀ NEL REGISTRO DORA
Pubblico	Sito, materiali commerciali, condizioni pubblicate, elenco dei subfornitori, security.txt	Pubblicazione approvata dal legale rappresentante	–
Interno	Procedure, immagini dei container, metriche di servizio senza dati dei Clienti	Solo personale e fornitori vincolati; nessuna pubblicazione	Low
Riservato	Dati degli utenti e degli studi, fatturazione, contratti, ticket, codice sorgente, i documenti di questo pacchetto	Accesso per necessità; cifratura in transito e a riposo; condivisione solo con chi è vincolato alla riservatezza	Medium
Strettamente riservato	Documenti ed elaborati delle pratiche, conversazioni con gli agenti, dati bancari e creditizi, dati giudiziari, atti penali e intercettazioni, segreti e chiavi, copie di sicurezza	Solo sulla piattaforma o nei servizi AWS indicati nell'inventario; mai su dispositivi personali, email, chat o strumenti non approvati; accesso del personale solo secondo P03 § 4.3, registrato	High

3 Regole

3.1 **Predefinito.** I dati dei Clienti sono «strettamente riservato» per impostazione predefinita, qualunque sia il loro contenuto: Trailgun non li ispeziona per declassarli.

3.2 **Prevalenza.** Il livello più alto prevale: un insieme che contiene un'informazione strettamente riservata è strettamente riservato.

3.3 **Etichetta.** I documenti di Trailgun riportano il livello in copertina o nel piede. I documenti di questo pacchetto sono «Riservato · per il Cliente»; le pagine pubbliche sono pubbliche.

3.4 **Trasmissione.** I dati strettamente riservati escono dalla piattaforma solo per azione dell'utente (download, esportazione, API, comunicazioni ai clienti dello studio che lo studio attiva) o verso i fornitori della politica P10, con i loro contratti. Le notifiche esterne (email, Telegram, SMS, WhatsApp) non portano dati delle pratiche: avvisano e rimandano all'app. Le ricerche sulle banche dati non portano nomi, codici fiscali, importi o dati delle pratiche.

3.5 **Conservazione e distruzione.** Secondo la politica P12. I supporti fisici sono di AWS, che li distrugge secondo le sue procedure attestate.

3.6 **Mascheramento.** Gli agenti lavorano sul testo integrale dei documenti, che è la ragione del servizio: la protezione dei dati delle pratiche è affidata ad accessi, cifratura, regione UE, nessun addestramento e regime rafforzato per il penale (politica P16), non alla pseudonimizzazione.

4 Classificare un'informazione nuova

1 Chi crea o riceve un'informazione nuova (un archivio, un registro, un tipo di file) ne individua il livello con la tabella del § 2; nel dubbio vale il livello più alto.

2 Se è un asset tecnico, il Responsabile della sicurezza lo aggiunge all'inventario (42) con livello, titolare e luogo.

3 Se contiene dati personali, il DPO lo riporta nel registro dei trattamenti (40) e verifica la base e la conservazione.

5 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
Classe degli asset	IN ESSERE livello, titolare e luogo di ogni asset	inventario 42, a ogni cambiamento
Notifiche senza dati delle pratiche	IN ESSERE testo generico con il collegamento all'app	verificabile su ogni canale
Sensibilità per il registro DORA	IN ESSERE corrispondenza con i valori del Reg. es. 2024/2956	scheda 16

6 Eccezioni e riferimenti normativi

Eccezioni secondo P01 § 8; nessuna eccezione declassa dati dei Clienti. Riferimenti: DORA art. 8; Reg. es. (UE) 2024/2956 (sensibilità dei dati, modello B_02.02); GDPR artt. 9, 10 e 32; ISO/IEC 27001:2022 controlli 5.12-5.14, 8.11 e 8.12.