Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO P14

VERSIONE 2.0 · DICEMBRE 2026

Politica di uso accettabile

Che cosa possono e non possono fare con sistemi e dati il personale di Trailgun e, per la parte che li riguarda, gli utenti degli studi: dispositivi, account, strumenti di IA, usi esclusi.

CODICE	TITOLARE	REVISIONE	STATO
P14 · POL-14	Responsabile della sicurezza	Annuale	al 01/12/2026

POLITICA P14 · POL-14

Politica di uso accettabile

Che cosa possono e non possono fare con sistemi e dati il personale di Trailgun e gli utenti degli studi.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P14 (POL-14)	Responsabile della sicurezza	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale	tutto il personale e i collaboratori; utenti e amministratori degli studi	Riservato · per il Cliente

DOCUMENTI COLLEGATI
P11, P13, P15, P16; inventario degli asset (42); documento 01 (Contratto di servizio); documento 19 (Informativa sull'IA ai clienti dello studio)

AMBITO
Dispositivi, account, posta, strumenti di sviluppo e di IA usati per lavorare per Trailgun; l'uso della piattaforma da parte degli utenti degli studi, insieme alle condizioni del contratto.

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
5.10, 6.7, 8.1	DORA art. 9; L. 132/2025 art. 13; AI Act art. 50

1 Scopo e ruoli

Le regole tecniche funzionano se le persone le rispettano. Il Responsabile della sicurezza fa conoscere questa politica con la formazione (politica P13) e ne verifica il rispetto; ogni persona ne risponde. Per gli utenti degli studi le regole valgono insieme al contratto di servizio.

2 Personale di Trailgun

- Dispositivi con disco cifrato, blocco automatico dello schermo e sistema aggiornato, registrati nell'inventario degli asset (42); autenticazione a più fattori su ogni account di lavoro.
- I dati dei Clienti si consultano solo sulla piattaforma o nei sistemi di AWS, e solo nei casi della politica P03 § 4.3; non si scaricano su dispositivi, non si inviano per email o chat, non si copiano in altri ambienti.
- Nessun dato dei Clienti, documento delle pratiche o segreto in strumenti di IA, traduttori o servizi web non approvati, compresi gli assistenti di programmazione.
- Vietato condividere credenziali, disattivare o aggirare un controllo, fare prove di sicurezza su production senza autorizzazione scritta, usare la piattaforma per scopi personali.
- Lavoro da remoto: reti fidate o VPN, nessuna sessione aperta su dispositivi altrui, attenzione a chi vede lo schermo.
- Ogni evento sospetto (email anomala, dispositivo perso, accesso inatteso) si segnala subito a security@trailgun.ai.
- L'uso dei sistemi aziendali può essere verificato nei limiti della L. 300/1970 e del GDPR, con informativa preventiva.

3 Utenti degli studi

- Ogni elaborato è una bozza che il professionista rivede prima di usarla; ogni segnalazione è una segnalazione con fonte, non una conclusione. La pagina dell'atto lo ricorda e i file prodotti dagli agenti portano la marcatura di contenuto generato con IA (politica P15).
- Le chat con l'assistente dell'atto e con l'assistenza dicono all'utente che sta parlando con un agente di IA; le mail che lo studio fa inviare in modalità automatica (richieste ai clienti, trattative) dicono ai destinatari che le ha preparate e inviate un agente di IA per conto dello studio.
- Si caricano solo i documenti necessari alla pratica; categorie particolari di dati solo nella misura necessaria.
- Credenziali e dispositivo di autenticazione sono personali; un dispositivo perso si segnala all'amministratore dello studio.
- L'avvocato informa i propri clienti dell'uso dell'IA (art. 13, c. 2, L. 132/2025); Trailgun fornisce il testo (documento 19).
- Non è consentito usare Trailgun per finalità escluse: uso da parte di un'autorità giudiziaria o per suo conto, valutazione del merito creditizio di persone fisiche, valutazione dell'affidabilità delle prove per conto di autorità di contrasto, profilazione di persone (politica P15).
- Per i fascicoli penali, la materia «penale» si sceglie nel modulo prima di caricare l'archivio, e nel titolo della pratica non si scrivono nomi di indagati o imputati (politica P16).

4 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
Presa visione del personale	IN ESSERE firmata con l'impegno di riservatezza	fascicolo della persona; formazione annuale (43)
Dispositivi	IN ESSERE cifratura, blocco, aggiornamenti	inventario 42; revisione trimestrale (44)
Avvisi di IA agli utenti e ai destinatari	IN ESSERE chat, pagina dell'atto, mail automatiche	verificabili nell'app

5 Eccezioni e riferimenti normativi

Eccezioni secondo P01 § 8. Riferimenti: DORA art. 9; L. 132/2025 art. 13 (uso dell'IA nelle professioni intellettuali: attività strumentali e di supporto, prevalenza del lavoro intellettuale, informazione al cliente); AI Act art. 50, par. 1; L. 300/1970; ISO/IEC 27001:2022 controlli 5.10, 6.7, 8.1.