Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO P16

VERSIONE 2.0 · DICEMBRE 2026

Politica sui fascicoli penali

Atti di indagine, intercettazioni e loro trascrizioni, dati relativi a reati: niente embeddings, registro di ogni accesso, nessun servizio fuori dall'UE, nessun dato nelle notifiche, cancellazione completa.

CODICE	TITOLARE	REVISIONE	STATO
P16 · POL-16	DPO e Responsabile della sicurezza	Annuale	al 01/12/2026

POLITICA P16 · POL-16

Politica sui fascicoli penali: regime rafforzato

Le regole in più per i fascicoli penali e misti: atti di indagine, intercettazioni e loro trascrizioni, dati relativi a reati.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P16 (POL-16)	DPO e Responsabile della sicurezza	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale	studi che trattano fascicoli penali; loro DPO; personale di Trailgun	Riservato · per il Cliente

DOCUMENTI COLLEGATI

P02, P03, P08, P11, P12, P15; documento 09 (AI Act e uso dell'IA nella professione); documento 50 (Supporto alla DPIA del Titolare); procedure 25 (Risposta agli incidenti) e 26 (Violazioni dei dati personali)

AMBITO

Ogni analisi del faldone per la quale l'avvocato ha scelto la materia «penale» nel modulo o che il classificatore della natura riconosce come penale o mista, con i suoi documenti, audio, trascrizioni, elaborati, domande e funzioni (matrice, timeline, grafo, scheda dell'imputato, iter delle intercettazioni).

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
5.12, 5.34, 8.3, 8.15	GDPR artt. 10, 35; art. 2-octies Codice privacy; artt. 114, 268, 269 c.p.p.

1 Perché un regime a sé

I fascicoli penali contengono dati relativi a reati (art. 10 GDPR), trattabili dall'avvocato per la difesa (art. 2-octies, c. 3, lett. e), Codice privacy), spesso voci e conversazioni di terzi, e atti la cui diffusione è vietata o limitata dalla disciplina processuale (in particolare artt. 114, 268 e 269 c.p.p.). Una loro esposizione ha impatto «molto alto» per definizione (politica P02) e nessun rischio sulla loro riservatezza si accetta oltre il livello medio.

2 Ruoli

Il DPO sorveglia l'applicazione di questa politica e approva, con istruzione scritta del Titolare, ogni eccezione; il Responsabile della sicurezza ne cura i controlli tecnici e il registro degli accessi del personale. L'avvocato dichiara la materia e decide che cosa caricare.

3 Regole

3.1 **Dichiarazione della materia.** L'avvocato sceglie la materia «penale» nel modulo prima di caricare l'archivio. Se non la sceglie, il fascicolo è trattato come penale quando il classificatore della natura lo riconosce penale o misto; la scelta esplicita fa valere il regime fin dal primo passo.

3.2 **Niente embeddings.** Sui fascicoli penali o misti non si costruisce l'indice semantico: la ricerca è solo per parole, anche per gli indici costruiti alla prima domanda.

3.3 **Registro degli accessi.** Ogni consultazione dei risultati (una all'ora per utente), domanda, analisi, confronto fra depositi, timeline, grafo e scheda dell'imputato generati diventa una riga del registro delle attività dello studio, con chi, quando e che cosa; il Titolare lo esporta. La scrittura del registro non blocca l'operazione se fallisce: l'errore va nei log.

3.4 **Modelli solo nell'UE.** Il testo dei fascicoli penali, come ogni altro testo, si elabora solo con Claude su Amazon Bedrock in una regione dell'UE; il fornitore del modello non riceve i dati e nessuno li usa per addestrare (politica P15).

3.5 **Audio e intercettazioni.** La trascrizione si fa con Amazon Transcribe a Francoforte, tramite un archivio temporaneo cifrato che scade entro 1 giorno; il riuso dei contenuti per i servizi di IA di AWS è escluso con una policy dell'organizzazione AWS di Trailgun.

3.6 **Nessun servizio fuori dall'UE.** Lo studio che tratta fascicoli penali lascia spento l'OCR di riserva negli Stati Uniti (DocuPipe, spento di default); le notifiche esterne non portano dati delle pratiche; le ricerche su One LEGALE non portano nomi, codici fiscali, importi o dati delle pratiche, per una regola in codice con test.

3.7 **Personale.** Nessun accesso del personale al contenuto se non su richiesta scritta dello studio o per un incidente, annotato nel registro degli accessi del personale. Il backoffice mostra i titoli delle pratiche: nel titolo lo studio non scrive nomi di indagati o imputati (politica P14).

3.8 **Segnalazioni, non conclusioni.** Le funzioni sul fascicolo (matrice, contraddizioni, filtro e scheda dell'imputato, iter delle intercettazioni) riportano ciò che gli atti dicono, con la fonte; non valutano la colpevolezza né il rischio che una persona commetta un reato.

3.9 **Cancellazione.** Alla cancellazione della pratica non resta nulla del fascicolo: documenti, audio, trascrizioni, testi, cache OCR, conversazioni con gli agenti e indici; le copie di sicurezza escono per rotazione entro 14 giorni (politica P12).

3.10 **Incidenti.** Un incidente che può toccare la riservatezza di un fascicolo penale si classifica «grave» (procedura 25) e si notifica al Titolare entro le 24 ore previste per le violazioni, senza attendere la certezza (procedura 26).

3.11 **DPIA.** Trailgun fornisce allo studio entro 10 giorni lavorativi le informazioni per la valutazione d'impatto, che il trattamento su larga scala di dati relativi a reati richiede (art. 35, par. 3, lett. b), GDPR), con il modello del documento 50.

4 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
Materia, niente embeddings, registro degli accessi	IN ESSERE regole in codice, con test	registro esportabile dallo studio
Modelli nell'UE; nessun servizio fuori dall'UE	IN ESSERE Bedrock in regione UE; DocuPipe spento di default; notifiche e ricerche senza dati	configurazione di production; registro 15
Cancellazione completa	IN ESSERE cache OCR e conversazioni comprese	a ogni cancellazione
Registro degli accessi del personale	IN ESSERE ogni accesso con richiesta e motivo	estratto al Titolare su richiesta

5 Eccezioni e riferimenti normativi

Nessuna eccezione alle regole 3.2-3.7 senza istruzione scritta del Titolare e parere del DPO. Riferimenti: GDPR artt. 10, 25, 32 e 35; art. 2-octies Codice privacy; artt. 114, 268 e 269 c.p.p.; AI Act art. 5, par. 1, lett. d); norme del Codice deontologico forense sul segreto e sulla riservatezza.