Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO 06



VERSIONE 2.0 · DICEMBRE 2026

Protezione dei dati personali

Il documento GDPR per l'ufficio privacy e il DPO di banche, intermediari, servicer e studi legali: ruoli, dati, fornitori, luoghi, misure dell'art. 32, conservazione, diritti, violazioni, con il registro dell'art. 30, par. 2, in sintesi e un supporto già compilato per la valutazione d'impatto.

RUOLO DI TRAILGUN	DATI A RIPOSO	MODELLI
Responsabile, art. 28	Germania · copie in Irlanda	Amazon Bedrock, regioni UE

QUADRO D'INSIEME

Chi decide, chi tratta, con quali garanzie

Il cliente decide quali documenti affidare e perché. Trailgun li lavora solo per svolgere il servizio, su istruzione del cliente, con dati, copie e modelli nelle regioni dell'Unione. Questo documento descrive le misure in essere al 01/12/2026 e la loro evidenza.

TITOLARE

Il cliente

La banca, l'intermediario, il servicer o lo studio legale. Sceglie pratiche, documenti e lavorazioni, ha la base giuridica, risponde agli interessati.

RESPONSABILE · ART. 28

Trailgun

Tratta i dati delle pratiche solo su istruzione, secondo il DPA (documento 07). È sub-responsabile quando il cliente tratta a sua volta per conto di altri.

TITOLARE AUTONOMO

Trailgun, per sé

Solo per gli account degli utenti, la sicurezza della piattaforma, l'assistenza, la fatturazione e i contatti commerciali.

Come si legge lo stato di ogni misura

IN ESSERE attivo in produzione, con evidenza mostrabile in audit

SU ISTRUZIONE eseguito da Trailgun quando il Titolare lo chiede

PERCORSO R tappa successiva, datata nel documento 12

I **Ruoli, dati e basi giuridiche** § 1-5
Trailgun e i contatti, ruoli lungo la catena, interessati e categorie, dati degli artt. 9 e 10.

II **Dove vanno i dati** § 6-9
Mappa per modulo, luoghi, sub-responsabili, trasferimenti con le loro valutazioni.

III **Misure tecniche e organizzative** § 10
Art. 32 GDPR, misura per misura.

IV **Conservazione, diritti, violazioni** § 11-13
Tempi di conservazione, supporto ai diritti degli interessati, gestione e tempi delle violazioni.

V **Scelte di progetto e garanzie** § 14-20
DPIA, protezione fin dalla progettazione, personale e segreto, IA, verifiche, assicurazioni, garanzie in essere.

All. **Registro art. 30, par. 2, e supporto alla DPIA** ALL. 1-2
Registro del responsabile in sintesi (completo nel foglio 40) e trattamenti propri; rischi e misure per la DPIA (modello compilabile 50).

PER IL DPO CHE HA CINQUE MINUTI

Le domande di sempre, con le risposte

24 ore
per notificare al Titolare una violazione dei dati personali

DE·IE
dati a riposo a Francoforte, copie di sicurezza in Irlanda

30/60 gg
preavviso su ogni sub-responsabile nuovo (60 per le funzioni DORA essenziali)

74 gg
al massimo dalla cessazione alla cancellazione, copie comprese

Dove sono i dati?

A riposo in Germania (AWS, Francoforte), con copie di sicurezza cifrate in Irlanda. I modelli Claude e gli embeddings girano su Amazon Bedrock nelle regioni dell'Unione; il codice rifiuta ogni regione fuori dall'UE.

Chi vede i documenti?

Gli utenti del cliente, secondo la visibilità che il cliente imposta per ogni suo cliente. Il personale di Trailgun li apre solo su richiesta o per un incidente, e ogni accesso va nel registro degli accessi del personale, che il Titolare può chiedere.

Se cancello, si cancella tutto?

Sì. La cancellazione di una pratica toglie documenti, testi, indici, elaborati, versioni, comunicazioni, attività, conversazioni con gli agenti e cache OCR dello studio; gli eventi di costo restano solo come importi, scollegati dai contenuti. Le copie escono per rotazione in 14 giorni.

Le violazioni?

Al Titolare entro 24 ore dalla conoscenza, con le informazioni dell'art. 33, par. 3. Al Titolare DORA anche la notifica iniziale dell'incidente TIC entro 2 ore. Rilevazione con sonda esterna ogni minuto, allarmi 24/7, CloudTrail e GuardDuty.

Il servicer lavora per un veicolo: e voi?

Se il cliente è responsabile per conto di un altro titolare, Trailgun è suo sub-responsabile: gli obblighi del DPA valgono verso il cliente, che ottiene l'autorizzazione a monte e riceve da Trailgun tutto ciò che serve per documentare la catena.

Quali fornitori sono fuori dall'UE?

Nessun modello: tutto su AWS nell'UE. Fuori dall'UE ci sono solo servizi accessori, ciascuno con la sua garanzia: Resend (società USA, invio dall'Irlanda), DocuPipe solo per lo studio che lo accende, canali di notifica senza dati delle pratiche (§§ 8 e 9).

Usate i nostri dati per addestrare modelli?

No. Né Trailgun né chi esegue i modelli addestra sui dati dei clienti: su Bedrock il produttore del modello non riceve i dati, e una policy di AWS Organizations esclude i contenuti di Textract, Transcribe e Bedrock dal miglioramento dei servizi di AWS (documento 60).

E i fascicoli penali?

Nessun indice di embeddings; ogni consultazione, domanda, analisi, timeline, grafo e scheda dell'imputato va nel registro degli accessi, consultabile dal Titolare. Il testo si elabora solo su Bedrock nell'UE. Regime rafforzato: politica P16.

Come si esce?

Dopo la cessazione, 30 giorni di accesso in sola lettura con esportazione, poi cancellazione entro i 30 giorni successivi con certificato scritto, e copie di sicurezza fuori rotazione entro altri 14 giorni. Per i clienti DORA, assistenza all'uscita fino a 12 mesi.

Chi è il DPO e a chi scrivo?

Un DPO esterno, [nome o società], nominato e comunicato al Garante, perché Trailgun tratta su larga scala dati relativi a reati per conto dei clienti (art. 37, par. 1, lett. c). Si scrive a privacy@trailgun.ai.

Ci aiutate con la DPIA?

Sì: informazioni entro 10 giorni lavorativi, l'Allegato 2 con descrizione, necessità, diciassette rischi con misure e rischio residuo, e il modello compilabile in Word (documento 50).

Certificazioni?

L'infrastruttura è certificata da AWS (ISO 27001, 27017, 27018, SOC 2, C5). Il percorso di Trailgun verso ISO/IEC 27001:2022 e il primo penetration test indipendente sono nel documento 12.

Con questo documento il DPO del cliente usa di solito anche: 07 Accordo sul trattamento dei dati · 15 Registro dei subfornitori · 40 Registro dei trattamenti del responsabile · 46 Mappa GDPR art. 28 · 50 Supporto alla DPIA · 26, 27, 28 Procedure per violazioni, richieste degli interessati e cancellazione · 61 Dichiarazione sulla localizzazione dei dati.

I · §§ 1-5

Ruoli, dati e basi giuridiche

Regolamento (UE) 2016/679 («GDPR») e d.lgs. 30 giugno 2003, n. 196 come modificato («Codice»). Le norme sono citate per articolo, paragrafo e lettera.

IN BREVE

- Per i dati delle pratiche il cliente è titolare e Trailgun è responsabile ai sensi dell'art. 28 GDPR, o sub-responsabile se il cliente tratta per conto di altri.
- Trailgun è titolare autonomo solo per account, sicurezza, assistenza, fatturazione e contatti commerciali.
- Nelle pratiche ci sono dati finanziari, dati relativi a reati (art. 10) e, occasionalmente, categorie particolari (art. 9), anche in registrazioni audio e intercettazioni.
- La base giuridica del trattamento delle pratiche è del Titolare; Trailgun gli dà gli elementi per documentarla.

1 Scopo, perimetro e stato del documento

1.1 Il documento descrive come la piattaforma Trailgun tratta i dati personali per conto delle banche, degli intermediari finanziari dell'art. 106 TUB, dei gestori di crediti e degli studi legali che la usano, e in quali casi Trailgun tratta dati per conto proprio. È scritto per l'ufficio privacy e il DPO del cliente: per la due diligence sul responsabile (art. 28, par. 1, GDPR), per la valutazione d'impatto (art. 35) e per il registro dei trattamenti (art. 30).

1.2 Descrive la piattaforma com'è al **01/12/2026**, sul codice in produzione e sulla configurazione dell'infrastruttura, rilette prima della pubblicazione di questa versione.

1.3 Ogni misura descritta è IN ESSERE, con un'evidenza mostrabile in audit. Le poche tappe successive (certificazioni, nuova piattaforma) sono richiamate con il loro codice PERCORSO R e datate nel documento 12, Percorso di certificazione e piattaforma.

1.4 Gli impegni (tempi di notifica, conservazione, copie di sicurezza, preavvisi, verifiche) sono gli stessi in tutti i documenti del pacchetto di conformità. L'Accordo sul trattamento dei dati (documento 07, il «DPA») li rende vincolanti; in caso di differenza prevale il DPA.

1.5 Le indicazioni sulle basi giuridiche e sulla valutazione d'impatto sono un supporto, non un parere: la responsabilità del trattamento resta del Titolare (artt. 5, par. 2, e 24 GDPR).

1.6 Il documento si aggiorna a ogni cambiamento rilevante della piattaforma, dei fornitori o degli impegni. Versione e data sono in copertina e a piè di pagina; le versioni precedenti si conservano e si forniscono su richiesta.

2 Trailgun e i contatti privacy

2.1 [Trailgun S.r.l.], con sede in [indirizzo], C.F. e P.IVA [...], Registro delle imprese e REA [...], PEC [...], LEI [...]. Legale rappresentante: **Franco Puppo**, CEO. Cofondatore: Alessandro Musella, avvocato, per il metodo e il legal design, senza ruoli esecutivi.

2.2 **Privacy**: privacy@trailgun.ai, per le richieste degli interessati, dei Titolari e dei loro DPO IN ESSERE.

2.3 **Sicurezza e violazioni**: security@trailgun.ai, presidiata 24 ore su 24 per le priorità 1, con risposta automatica che indica il numero di reperibilità [+39 ...] IN ESSERE.

2.4 **Responsabile della protezione dei dati**: [DPO esterno: nome o società], dpo@[...] IN ESSERE. La designazione è obbligatoria anche per il responsabile quando le sue attività principali consistono nel trattamento su larga scala di categorie particolari o di dati relativi a reati (art. 37, par. 1, lett. c, GDPR): è il caso di Trailgun, che tratta fascicoli civili e penali per conto dei clienti. Il DPO è esterno (art. 37, par. 6); i suoi contatti sono pubblicati e comunicati al Garante (art. 37, par. 7).

2.5 **Responsabile della sicurezza**: Franco Puppo, CEO; un responsabile dedicato è la tappa R13 del Percorso. **Referente per la conformità IA**: [nome].

2.6 Trailgun è stabilita in Italia: l'autorità di controllo è il Garante per la protezione dei dati personali. Non serve un rappresentante ai sensi dell'art. 27 GDPR.

3 I ruoli lungo la catena

3.1 **Il cliente è titolare** (art. 4, n. 7, GDPR) dei dati personali contenuti nei documenti delle pratiche e negli elaborati: decide quali pratiche e quali documenti affidare a Trailgun, quali lavorazioni avviare, quali utenti vi accedono e quando cancellare. Lo studio legale è titolare dei dati che tratta per i suoi incarichi, come indicano le Linee guida EDPB 07/2020; la banca e l'intermediario lo sono per i rapporti e i crediti che gestiscono.

3.2 **Trailgun è responsabile** (art. 4, n. 8, e art. 28 GDPR) secondo il DPA. Le scelte tecniche e organizzative non essenziali (infrastruttura, modelli, misure, fornitori) spettano a Trailgun nei limiti del DPA, come ammettono le stesse Linee guida.

3.3 **Catene più lunghe.** Il servicer di una cartolarizzazione (legge 30 aprile 1999, n. 130) o il gestore che lavora per conto di una banca può trattare i dati come responsabile del proprio mandante. In quel caso Trailgun è sub-responsabile (art. 28, par. 4, GDPR): gli obblighi del DPA valgono verso il cliente, che deve avere dal proprio titolare l'autorizzazione a ricorrere a Trailgun e ai suoi sub-responsabili (DPA, art. 2.4). Trailgun fornisce al cliente tutto ciò che gli serve per documentare la catena (Parere EDPB 22/2024).

3.4 **Trailgun è titolare autonomo** soltanto per: **(a)** gli account degli utenti e l'autenticazione; **(b)** la sicurezza della piattaforma e i suoi registri tecnici; **(c)** la gestione del rapporto di assistenza; **(d)** la fatturazione e l'amministrazione del contratto; **(e)** i contatti commerciali con banche, intermediari e studi, senza newsletter né comunicazioni promozionali in assenza di un consenso specifico; **(f)** il sito trailgun.ai, che non usa cookie né strumenti di analisi. Il registro di questi trattamenti è nell'Allegato 1, parte B. Il contenuto dei ticket di assistenza che riporta dati delle pratiche resta trattato per conto del Titolare.

3.5 **Che cosa vede lo staff della piattaforma.** Gli amministratori della piattaforma vedono nel pannello interno studi, utenti, costi, l'elenco delle pratiche e le ricerche recenti di tutti gli studi: metadati come titoli, stati e costi, non il contenuto, perché il controllo di visibilità vale anche per loro IN ESSERE. I titoli delle pratiche possono contenere nomi: chi vuole minimizzare usa titoli neutri. Gli operatori dell'assistenza vedono solo ticket e base di conoscenza.

3.6 **Che cosa Trailgun non fa.** Non raccoglie dati presso gli interessati e non li arricchisce con fonti esterne di propria iniziativa; scrive ai clienti del Titolare o alle controparti solo con le comunicazioni che il Titolare attiva; non fa profilazione né decisioni basate unicamente su un trattamento automatizzato (art. 22 GDPR); non vende né cede dati.

4 Interessati e categorie di dati

4.1 **Interessati.** Clienti del Titolare e loro rappresentanti; debitori, debitori ceduti, garanti e fideiussori; controparti e loro difensori; parti di contratti e trattative; curatori, commissari e altri organi delle procedure; indagati, imputati, persone offese, testimoni e altri soggetti di procedimenti penali, comprese le persone intercettate; dipendenti e collaboratori del Titolare; ogni altra persona citata nei documenti. Possono esserci minori e persone in condizioni di vulnerabilità economica.

4.2 **Dati comuni.** Anagrafici e di contatto; codici fiscali e documenti d'identità; dati di rapporti contrattuali e bancari (contratti, fatture, estratti conto, piani di ammortamento, garanzie, segnalazioni); dati economici, patrimoniali e fiscali; dati di procedure giudiziarie civili, concorsuali, amministrative e tributarie; contenuto di email e messaggi; registrazioni audio e trascrizioni.

4.3 **Dati relativi a condanne penali e reati** (art. 10 GDPR): negli atti dei fascicoli penali e, a volte, in quelli civili (querele, sentenze, misure). Fuori dal controllo dell'autorità pubblica il loro trattamento è consentito solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento (art. 2-octies, comma 1, del Codice); per l'avvocato vale il comma 3, lett. e), «l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria».

4.4 **Categorie particolari** (art. 9 GDPR): Trailgun non le cerca, ma possono comparire nei documenti (cartelle cliniche in una causa di danni, dati sindacali, contenuto di conversazioni intercettate). Per l'avvocato la condizione è l'art. 9, par. 2, lett. f). La distinzione dei parlanti nelle trascrizioni separa le voci dentro una registrazione e non serve a identificare le persone: non è un trattamento di dati biometrici ai sensi dell'art. 4, n. 14.

4.5 **Larga scala.** Un data tape di una cartolarizzazione o un lotto di pratiche possono riguardare migliaia di debitori. Se il trattamento è su larga scala lo valuta il Titolare, con i criteri delle linee guida EDPB sul DPO e sulla DPIA; l'Allegato 2 lo aiuta.

4.6 **Dati degli utenti** (Trailgun titolare): email, che è anche il nome utente, ruolo, studio, preferenze, eventuale chat Telegram collegata, attività sulla piattaforma. **Dati di fatturazione dello studio**: dati fiscali e, per la fatturazione a consumo, il riferimento Stripe e le ultime quattro cifre della carta.

4.7 **Dati tecnici.** Log di accesso senza corpo delle richieste né token; log dell'applicazione con identificativi, nomi di file ed errori, mai testo dei documenti; i nomi dei file possono contenere nomi di persone e sono trattati come dati personali. Eventi di costo con modello, agente, quantità e importi, mai il testo dei documenti IN ESSERE.

5 Basi giuridiche

5.1 **Del Titolare, per i dati delle pratiche.** Le indicazioni più comuni, da valutare caso per caso:

- **Studio legale**: art. 6, par. 1, lett. b) per il mandato e lett. f) per la tutela dei diritti del cliente verso i terzi; art. 9, par. 2, lett. f); art. 2-octies, comma 3, lett. e), del Codice; Regole deontologiche per le investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria.
- **Banca, intermediario, servicer**: art. 6, par. 1, lett. b) per i rapporti con il debitore, lett. c) per gli obblighi di vigilanza e lett. f) per il recupero del credito. Per i dati relativi a reati trattati fuori da un giudizio la condizione dell'art. 2-octies va valutata caso per caso: nel testo vigente non c'è una lettera dedicata al recupero crediti.

5.2 **Di Trailgun, come responsabile.** Nessuna base propria: tratta su istruzione documentata (art. 28, par. 3, lett. a, e art. 29 GDPR) e la liceità discende da quella del Titolare.

5.3 **Di Trailgun, come titolare.** Account e sicurezza: legittimo interesse a eseguire il contratto con lo studio e a proteggere la piattaforma (art. 6, par. 1, lett. f), o esecuzione del contratto quando l'utente è la parte (lett. b). Fatturazione: obbligo di legge (lett. c) e contratto (lett. b). Assistenza: contratto (lett. b). Contatti commerciali: misure precontrattuali (lett. b) e legittimo interesse (lett. f); comunicazioni promozionali solo con il consenso (lett. a).

5.4 **Informazione agli interessati.** La dà il Titolare (artt. 13 e 14 GDPR), nei limiti dell'art. 14, par. 5, lett. b) e d), per i dati soggetti a segreto professionale. Trailgun fornisce la descrizione del trattamento da riportare nell'informativa. L'informazione ai clienti sull'uso di sistemi di intelligenza artificiale prevista dall'art. 13, comma 2, della legge 23 settembre 2025, n. 132, è del professionista: Trailgun gliene fornisce il modello compilabile (documento 19).

II · § 6

Mappa dei dati per modulo

Che cosa entra, chi lo elabora e che cosa resta, per ciascuna parte della piattaforma. I fornitori sono quelli del § 8. Le funzioni nuove sono opzioni: spente, il flusso resta quello di prima. Il registro completo per modulo è il foglio 40.

MODULO	DATI IN INGRESSO	ELABORAZIONE E FORNITORI	CHE COSA RESTA	ACCORGIMENTI
Ricorso per decreto ingiuntivo	Archivio del credito: contratti, fatture, estratti conto, solleciti, anagrafiche di debitore e garanti	OCR (Textract), agenti su Bedrock UE, raccolta dati, redazione e controllo; verifica giurisprudenziale su One LEGALE se attivata	Documenti, testi, dati con fonte, atto e versioni, faldone	Ogni dato rimanda a documento e pagina o è «N/D»; verifica giurisprudenziale spenta di default
Assessment (due diligence su crediti ceduti)	Faldone del credito ceduto; questionario del template	Un agente per documento e un agente di controllo per domanda, su Bedrock UE	Risposte, note e fonti per domanda	Il questionario si congela sulla pratica alla creazione
Insinuazione al passivo	Titoli del credito, atti della procedura, dati del curatore	Motore a playbook su Bedrock UE; OCR	Domanda, allegati, dati con fonte	–
Escussione delle garanzie pubbliche (Fondo PMI, SACE, ISMEA)	Pratica di finanziamento e garanzia, dati dell'impresa e dei garanti	Motore a playbook su Bedrock UE; visure via Openapi se richieste	Richiesta di escussione e allegati	Visure solo su richiesta dell'utente
Remediation del data tape	Data tape della cartolarizzazione con dati per debitore e per rapporto, documenti di supporto	Motore a playbook e controlli in codice; Bedrock UE	Tape corretto, rilievi con fonte	Possibile larga scala: da considerare nella DPIA del Titolare
Analisi del faldone e domande	Fascicolo intero (anche penale), domande dell'avvocato	Estesa: il modello legge tutto il fascicolo, tenuto nella cache del prompt di Bedrock per un'ora, nella stessa regione. Veloce: embeddings Amazon Titan su Bedrock UE e ricerca lessicale locale	Relazione, domande e risposte con documento e pagina	Sui fascicoli penali o misti niente embeddings: solo ricerca per parole
Funzioni sul fascicolo	Testi del fascicolo	Matrice affermazioni e fonti, timeline, grafo delle relazioni, contraddizioni, calcoli, filtro e scheda dell'imputato; Bedrock UE e calcolo in codice	Segnalazioni con fonte	Ogni uscita è una segnalazione, mai una conclusione; sul penale ogni consultazione, analisi, timeline, grafo e scheda va nel registro degli accessi
Audio e intercettazioni	Registrazioni, anche intercettazioni; documenti dell'iter (RIT)	Trascrizione con Amazon Transcribe a Francoforte, parlanti distinti; poi Bedrock UE	Trascrizioni, prospetto dell'iter	File temporaneo su S3 cancellato a fine analisi, scadenza 1 giorno
Trattative (affitto di ramo d'azienda)	Bozze, messaggi di approvatori interni, controparti, notaio	Agenti su Bedrock UE; email con Resend a indirizzi dedicati della trattativa	Versioni, approvazioni, messaggi	Spente per studio di default; nella modalità automatica la mail dichiara l'uso dell'IA
Revisione in Word	Atto in DOCX	Dal browser dell'utente al OneDrive o SharePoint del Titolare; il file rivisto torna e si converte in PDF/A sul server (LibreOffice)	Versione rivista e PDF	Trailgun non vede le credenziali Microsoft; Microsoft non è suo sub-responsabile
Ricerca fonti e verifica giurisprudenziale	Domanda giuridica	Il modello compone le ricerche; un browser automatico interroga One LEGALE con l'account di Trailgun	Fonti e massime trovate	Una regola in codice, con test, toglie nomi, codici fiscali, importi e dati delle pratiche dalle ricerche

MODULO	DATI IN INGRESSO	ELABORAZIONE E FORNITORI	CHE COSA RESTA	ACCORGIMENTI
Raccoglitore dati	Documenti della pratica	Agenti su Bedrock UE	Anagrafiche di soggetti e rapporti con le fonti	Acceso di default; solo dati presenti nei documenti, nessuna fonte esterna
Comunicazioni e canali d'ingresso	Richieste di documenti ai clienti del Titolare e risposte; mail alle caselle dello studio; chiamate API	Resend (invio e ricezione); smistatore su Bedrock UE per le caselle; API con chiavi dello studio	Messaggi e allegati nella pratica	Mail da mittenti non ammessi rifiutate; arrivi in quarantena finché un utente non li approva o rifiuta
Assistenza	Domande in chat, ticket e allegati	Agente di supporto su Bedrock UE, dalla base di conoscenza	Conversazioni e ticket	Gli operatori vedono solo ticket e base di conoscenza; la chat dichiara che risponde un assistente di IA
Memoria dello studio	Correzioni dell'avvocato che valgono per i prossimi atti	Assistente dell'atto; conferma dell'utente e, per lo studio, di un admin	Regola nei testi aggiuntivi dello studio	Resta nello studio, mai nei testi di Trailgun
Notifiche e richiesta di attenzione	Avviso, link, messaggio facoltativo del collega	App; email (Resend); Telegram; SMS e WhatsApp (Twilio)	Notifiche nell'app	Fuori dall'app solo un avviso generico e il link, senza dati delle pratiche
Fatturazione	Dati di fatturazione dello studio, costi per pratica	Stripe per la carta dello studio, con la fatturazione a consumo	Fatture, rendiconti	Costi senza testo dei documenti

§ 7

Dove sono i dati e dove passano

Luoghi di conservazione e di elaborazione. La Dichiarazione sulla localizzazione dei dati nell'Unione è il documento 61.

CHE COSA	DOVE	GARANZIE
Dati a riposo (database, documenti, elaborati)	Germania, AWS eu-central-1 (Francoforte), su un disco EBS cifrato	IN ESSERE più zone di disponibilità: PERCORSO R12
Copie di sicurezza	Francoforte e, per la produzione, Irlanda (AWS eu-west-1), cifrate, 14 giorni	IN ESSERE
File temporanei per OCR e trascrizione	S3 a Francoforte, cancellati a fine analisi, scadenza 1 giorno	IN ESSERE
OCR e trascrizione	Amazon Textract e Transcribe a Francoforte	IN ESSERE opt-out dal miglioramento dei servizi di IA di AWS con policy di AWS Organizations
Modelli linguistici	Claude di Anthropic su Amazon Bedrock, regione di Francoforte (UE); richieste firmate dal ruolo dell'istanza	IN ESSERE regioni fuori dall'UE rifiutate dal codice; il produttore del modello non riceve i dati
Embeddings (ricerca veloce)	Amazon Titan Text Embeddings V2 su Bedrock, regione UE; mai sui fascicoli penali	IN ESSERE
OCR di riserva	DocuPipe, Stati Uniti, solo per lo studio che lo accende	IN ESSERE spento di default; clausole tipo e valutazione del trasferimento
Email	Resend: invio e ricezione su AWS SES in Irlanda; società statunitense	IN ESSERE DPA, Data Privacy Framework verificato, valutazione del trasferimento
Notifiche Telegram, SMS, WhatsApp	Fornitori fuori dall'UE scelti dall'utente	IN ESSERE solo avviso generico e link, nessun dato delle pratiche

CHE COSA	DOVE	GARANZIE
Firma e visure	Openapi e Namirial, Italia, ambiente di produzione	IN ESSERE DPA firmato
Banca dati giuridica	One LEGALE (Wolters Kluwer Italia), Italia: riceve le stringhe di ricerca, senza nomi né dati delle pratiche	IN ESSERE regola in codice con test; DPA firmato
Revisione in Word	Tenant Microsoft del Titolare, secondo il suo contratto con Microsoft	–

§ 8

Sub-responsabili e altri fornitori

Tutti i fornitori della piattaforma in produzione. È lo stesso elenco dell'Allegato 3 del DPA e del Registro dei subfornitori (documento 15), pubblicato su https://trailgun.ai/subprocessors.

FORNITORE	ATTIVITÀ	DATI	LUOGO	GARANZIE
Amazon Web Services EMEA SARL, Lussemburgo	Infrastruttura (EC2, EBS, S3, ECR, SSM, CloudWatch, CloudTrail, Route 53, KMS, DLM), login (Cognito), email di Cognito (SES), OCR (Textract), trascrizione (Transcribe), modelli ed embeddings (Bedrock)	Tutti i documenti, gli elaborati e i dati degli utenti	Germania; copie in Irlanda; Bedrock nelle regioni UE	IN USO DPA di AWS firmato; account dedicato e intestato a Trailgun; opt-out dei servizi di IA; certificazioni AWS
Plus Five Five, Inc. (Resend)	Email in uscita (richieste ai clienti, trattative, notifiche) e risposte in entrata	Indirizzi, oggetto, testo; allegati delle risposte (fino a 25 MB, 20 per messaggio); contratto e report allegati alle email delle trattative	Invio su SES in Irlanda; società USA	IN USO DPA firmato; conservazione presso Resend [giorni]; Data Privacy Framework verificato
Wolters Kluwer Italia S.r.l. (One LEGALE)	Banca dati giuridica, interrogata con l'account di Trailgun	Stringhe di ricerca senza nomi, codici fiscali, importi o dati delle pratiche	Italia	IN USO DPA firmato
Openapi S.p.A. con **Namirial S.p.A.**	Firma qualificata e visure camerali, su richiesta del Titolare	PDF da firmare, dati del firmatario; P.IVA o C.F. delle imprese	Italia	IN USO DPA firmato
Hoss Inc. (DocuPipe)	OCR di riserva, solo per lo studio che lo accende	Il singolo file che Textract non legge	Stati Uniti	OPZIONE spenta di default; DPA firmato; conservazione [giorni]; clausole tipo
Telegram	Notifiche agli utenti che collegano la chat	Avviso generico e link, senza dati delle pratiche	Fuori dall'UE	OPZIONE DELL'UTENTE
Twilio Inc.	SMS e WhatsApp agli utenti che li scelgono	Numero dell'utente, avviso e link	Stati Uniti	OPZIONE DELL'UTENTE
Stripe	Carta e addebiti dello studio, con la fatturazione a consumo	Dati di pagamento dello studio, non dati delle pratiche	UE e Stati Uniti	Titolare autonomo per i dati di pagamento
Google (Workspace)	Caselle email delle persone di Trailgun (per esempio info@, privacy@, security@)	Email che clienti e studi scrivono a quegli indirizzi, con eventuali allegati	–	Corrispondenza di Trailgun; non riceve dati dalla piattaforma

Fornitori che non ricevono dati personali dei clienti. GitHub (codice e integrazione continua, Stati Uniti), Let's Encrypt (certificati), Docker Hub e npm (immagini e pacchetti). **Microsoft**: l'app multi-tenant di Trailgun serve solo al login dal browser per la revisione in Word; il file va al tenant del Titolare e Microsoft non riceve dati da Trailgun. **Anthropic** produce i modelli Claude ma non è un sub-responsabile: i modelli girano su Amazon Bedrock e Anthropic non riceve i dati.

Catena a valle. Trailgun fornisce su richiesta l'identità dei fornitori a valle di ciascun sub-responsabile, come chiede il Parere EDPB 22/2024. Ogni fornitore si valuta prima dell'ingaggio e ogni anno (procedura 29), con DPA, certificazioni, regioni e garanzie di trasferimento nel Registro dei subfornitori (documento 15).

§ 9

Trasferimenti e dipendenze fuori dall'Unione

Archivi, copie, modelli ed embeddings sono nell'Unione. Escono solo i flussi accessori qui sotto, ciascuno con la sua base e, dove serve, la valutazione d'impatto del trasferimento svolta.

FORNITORE	CHE COSA ESCE	BASE DEL TRASFERIMENTO	COME SI LIMITA
Resend	Email delle comunicazioni attivate dal Titolare e risposte; accesso eventuale della società statunitense	Data Privacy Framework UE-USA (certificazione verificata), con clausole contrattuali tipo come garanzia sostitutiva; valutazione del trasferimento svolta	Le comunicazioni partono solo se lo studio le attiva; la funzione si può spegnere
DocuPipe	Singoli file non letti da Textract	Clausole contrattuali tipo, modulo 3; valutazione del trasferimento svolta	Solo per lo studio che accende l'opzione, spenta di default
Telegram, Twilio	Avviso generico e link, identificativo del canale scelto dall'utente	Nessun dato delle pratiche; canale scelto dall'utente per sé	L'utente collega o scollega il canale in ogni momento
Stripe	Dati di pagamento dello studio	Garanzie di Stripe come titolare autonomo	Nessun dato delle pratiche
AWS	Nessun trasferimento previsto; possibile accesso per assistenza tecnica del gruppo e accesso di autorità statunitensi alla capogruppo	Data Privacy Framework e clausole contrattuali tipo dell'AWS GDPR DPA	Regioni UE; cifratura; chiavi KMS gestite da Trailgun con la nuova piattaforma (Percorso R12)

9.1 Ogni trasferimento si fonda su una decisione di adeguatezza (art. 45 GDPR) o sulle clausole contrattuali tipo della Decisione di esecuzione (UE) 2021/914 (art. 46), con le misure supplementari che servono secondo le Raccomandazioni EDPB 01/2020.

9.2 Il Data Privacy Framework UE-USA (Decisione di esecuzione (UE) 2023/1795) è oggetto di contenzioso davanti alle corti dell'Unione: per questo le clausole contrattuali tipo restano sempre la garanzia sostitutiva.

9.3 Il rischio residuo è l'accesso di autorità di paesi terzi presso fornitori con capogruppo statunitense, come AWS. Le misure: dati e modelli nelle regioni UE, cifratura a riposo e in transito, contestazione di ogni richiesta non fondata su un accordo internazionale (art. 48 GDPR), informazione al Titolare se la legge lo consente (DPA, art. 14). AWS EMEA SARL è tra i fornitori terzi critici designati dalle autorità europee il 18/11/2025: il Titolare soggetto a DORA lo considera nella valutazione di concentrazione.

9.4 Le valutazioni d'impatto dei trasferimenti verso Resend e DocuPipe si forniscono su richiesta a privacy@trailgun.ai e si mostrano in sede di audit.

III · § 10

Misure tecniche e organizzative (art. 32 GDPR)

Ordinate secondo l'art. 32, par. 1: cifratura (lett. a), riservatezza, integrità, disponibilità e resilienza (lett. b), ripristino (lett. c), verifica dell'efficacia (lett. d). È lo stesso contenuto dell'Allegato 2 del DPA; il dettaglio tecnico è nel documento 05, Sicurezza delle informazioni.

AREA	MISURA	STATO
Cifratura a riposo (lett. a)	Disco dei dati e disco di sistema cifrati con AWS KMS (AES-256); copie di sicurezza cifrate in entrambe le regioni; archivio temporaneo S3 con cifratura lato server, accesso pubblico bloccato, solo TLS, scadenza 1 giorno. Nessuna cifratura applicativa dei database e dei file oltre a quella del volume.	IN ESSERE chiavi gestite da Trailgun: PERCORSO R12
Cifratura in transito (lett. a)	HTTPS con certificati Let's Encrypt rinnovati in automatico, reindirizzamento da HTTP a HTTPS, HTTP/3, TLS 1.2 e 1.3; verso i fornitori sempre HTTPS. HSTS di 1 anno e intestazioni di sicurezza (CSP, X-Content-Type-Options, Referrer-Policy, frame-ancestors).	IN ESSERE
Pseudonimizzazione e minimizzazione (lett. a)	Eventi di costo senza testo dei documenti; chiavi API conservate solo come impronta SHA-256; password mai conservate da Trailgun (protocollo SRP di Cognito); ricerche giuridiche senza dati delle pratiche; notifiche esterne senza dati delle pratiche. Gli elaborati portano dati in chiaro perché servono all'atto: la pseudonimizzazione dei contenuti non è applicabile allo scopo.	IN ESSERE
Accesso degli utenti (lett. b)	Solo su invito; Amazon Cognito con SRP; secondo fattore TOTP obbligatorio per tutti; password di almeno 10 caratteri con maiuscole, minuscole e cifre; password temporanea valida 7 giorni; nessuna rivelazione dell'esistenza di un account; protezione dalla cancellazione del pool. Ogni richiesta alle API verificata sul token (firma, scadenza, destinatario) e confrontata con l'utente.	IN ESSERE
Sessioni	Token d'identità a scadenza breve ([1 ora] sul client di produzione). La disattivazione dell'account dal pannello blocca subito i nuovi accessi; una sessione già aperta dura fino alla scadenza del token.	IN ESSERE
Ruoli e permessi	Ruoli di studio admin, membro, operator (porta avanti le pratiche, non ne crea) e viewer (sola lettura), imposti lato server; permessi concessi a singoli membri (richiesta di attenzione, amministrazione).	IN ESSERE
Separazione fra studi	Un solo database per tutti gli studi, con separazione logica: ogni interrogazione sui dati di un cliente passa da un unico predicato di visibilità, con visibilità per cliente (tutto lo studio, solo chi l'ha creato, persone selezionate) e test dedicati. Cache OCR, cache del layout e deduplica legate allo studio, mai condivise.	IN ESSERE
Separazione degli ambienti	Sviluppo, collaudo e produzione con macchina, disco, segreti, log e pool di login propri; fuori produzione servizi esterni finti e il pool dello stack imposto dallo script di rilascio.	IN ESSERE
Fascicoli penali	Nessun indice di embeddings; registro di ogni consultazione (una all'ora per utente), domanda, analisi, confronto fra depositi, timeline, grafo e scheda dell'imputato, consultabile dal Titolare; testo elaborato solo su Bedrock nell'UE. Politica P16.	IN ESSERE
Accesso amministrativo all'infrastruttura	Nessuna porta SSH; in ingresso solo 80 e 443; amministrazione con SSM Session Manager e Run Command, sessioni registrate; metadati dell'istanza solo IMDSv2; ruolo dell'istanza a privilegi limitati; credenziali amministrative solo temporanee (IAM Identity Center); CloudTrail su tutte le regioni, 12 mesi.	IN ESSERE
MFA amministrativa	Secondo fattore obbligatorio su AWS (root, Identity Center e console), GitHub con l'obbligo per l'intera organizzazione, Google Workspace, Stripe, Resend e ogni console di fornitore.	IN ESSERE

AREA	MISURA	STATO
Personale e accesso ai contenuti	Accesso ai contenuti solo su richiesta del Titolare o per un incidente, registrato nel registro degli accessi del personale; impegno scritto di riservatezza e designazione al trattamento (art. 29 GDPR e art. 2-quaterdecies del Codice); revoca degli accessi entro 24 ore dalla cessazione di una persona; revisione trimestrale degli accessi privilegiati (procedura 22, modello 44).	IN ESSERE
Formazione	Formazione su sicurezza e privacy all'ingresso e ogni anno; alfabetizzazione sull'IA ogni anno (art. 4 AI Act); verifica dei precedenti per chi accede alla produzione, nei limiti dell'art. 8 dello Statuto dei lavoratori e dell'art. 10 GDPR. Registro della formazione: documento 43.	IN ESSERE
Segreti	Credenziali dei servizi in SSM Parameter Store (SecureString), mai nel codice, nell'immagine o nel modello dell'infrastruttura; sul server file di configurazione leggibile solo dal servizio; in produzione nessuna variabile «finta»; scansione dei segreti su tutta la storia del codice a ogni verifica. Rotazione dei segreti dei fornitori ogni 12 mesi e subito dopo un sospetto o l'uscita di una persona con accesso.	IN ESSERE
Ingresso dei dati	Limiti su numero (5.000 voci) e dimensione degli archivi contro gli zip malevoli; webhook in entrata verificati (Svix con tolleranza di 5 minuti, o segreto condiviso; senza segreto la rotta risponde 503); webhook in uscita firmati HMAC-SHA256 con marca temporale; chiavi API con limite di 120 richieste al minuto. I file si aprono solo sul server, in un container senza privilegi.	IN ESSERE filtro WAF: PERCORSO R12
Host e container	Immagine del sistema operativo fissata e aggiornata ogni mese; scansione delle immagini dei container al caricamento; container dell'app eseguito senza privilegi di root; immagine del proxy fissata a una versione.	IN ESSERE
Integrità degli elaborati (lett. b)	Ogni dato rimanda a documento e pagina o è «N/D»; ogni versione dell'atto conserva autore e motivo e il testo si scrive da un solo punto del codice; impronte SHA-256 dei file del faldone e del pacchetto di deposito.	IN ESSERE
Registri (lett. b)	Log di accesso HTTP e log dell'applicazione su CloudWatch, 90 giorni, senza corpo delle richieste, token o testo dei documenti; log di sicurezza e amministrazione (CloudTrail su tutte le regioni con convalida dell'integrità, sessioni SSM, accessi al pannello) 12 mesi; registro delle attività per studio, consultabile dall'admin; registro degli accessi ai fascicoli penali. Orologi sincronizzati con Amazon Time Sync.	IN ESSERE
Rilevazione (lett. b)	Sonda esterna ogni minuto; allarmi 24/7 su salute, disco, CPU, memoria, errori 5xx e scadenza dei certificati; Amazon GuardDuty; pagina «Sistema» del pannello.	IN ESSERE
Disponibilità e resilienza (lett. b)	Una istanza per ambiente a Francoforte, infrastruttura come codice, ricostruibile; il rilascio non parte se ci sono lavorazioni del modulo in corso, quelle in coda ripartono da sole. Disponibilità del 99,5% mensile (99,8% in orario lavorativo), misurata dalla sonda.	IN ESSERE più zone: PERCORSO R12
Copie di sicurezza (lett. c)	Snapshot giornaliero del disco dati alle 02:00 UTC, 14 conservati, copia cifrata in Irlanda conservata 14 giorni; snapshot prima di ogni rilascio di produzione, conservato 14 giorni; copia del database prima di ogni migrazione, ultime 5.	IN ESSERE copie ogni 4 ore: PERCORSO R01
Ripristino (lett. c)	RPO 24 ore; RTO 8 ore per guasto dell'istanza, del disco o della zona. Runbook scritto (procedura 30); prova automatica a ogni verifica della CI e prova trimestrale sullo snapshot reale, in ambiente isolato, con verbale e RTO misurato (programma 31).	IN ESSERE ripristino regionale: PERCORSO R03
Sviluppo e rilasci	Branch di ambiente protetti; verifica obbligatoria prima di ogni rilascio, anche manuale (controllo dei tipi, test unitari, test end-to-end, scansione dei segreti, prova di ripristino); integrazione continua senza chiavi AWS (OIDC), un ruolo per ambiente assumibile solo dal suo ramo; migrazioni del database numerate e solo in avanti; funzioni nuove come opzioni.	IN ESSERE

AREA	MISURA	STATO
Vulnerabilità (lett. d)	Dependabot settimanale su dipendenze, immagini e azioni; scansione delle immagini; correzioni entro 72 ore (critiche, o sfruttate attivamente), 7 giorni (alte), 30 (medie), 90 (basse) dalla disponibilità della correzione; segnalazione responsabile su https://trailgun.ai/security.	IN ESSERE scansione esterna mensile: PERCORSO R05
Verifica dell'efficacia (lett. d)	Prove di ripristino trimestrali; test automatici a ogni rilascio; revisione trimestrale degli accessi; riesame annuale delle politiche e del registro dei rischi; audit del Titolare.	IN ESSERE penetration test: PERCORSO R06
Fornitori	DPA scritti con ogni sub-responsabile, con obblighi non meno rigorosi del DPA (art. 28, par. 4); opt-out dai servizi di IA di AWS; valutazione prima dell'ingaggio e ogni anno.	IN ESSERE
Notifiche esterne	Le notifiche fuori dall'app portano solo un avviso generico e il link; il contenuto si legge in app, dopo il login.	IN ESSERE

IV · § 11

Conservazione e cancellazione

Durante il contratto decide il Titolare: nessuna scadenza automatica. Qui, archivio per archivio, quanto resta. Politica P12, procedura 28.

DATO	CONSERVAZIONE	CANCELLAZIONE
Pratiche, documenti originali, testi, indici, elaborati, versioni	Finché il Titolare non cancella la pratica o il cliente; le pratiche archiviate restano	Con la pratica; a fine contratto con lo studio
Conversazioni con gli agenti	Con la pratica	Con la pratica e con lo studio
Cache OCR e del layout	Dello studio, mai condivisa	Con la pratica
Archivio delle fonti di One LEGALE	Testi giuridici pubblici, senza dati delle pratiche	A fine contratto, nella cancellazione dello studio
Registro delle attività, log degli accessi penali	Per tutta la durata del contratto, esportabili dal Titolare in CSV	Con lo studio alla cessazione
Eventi di costo	Importi per la fatturazione, scollegati dai contenuti	Dati di fatturazione 10 anni (art. 2220 c.c.)
File temporanei OCR e trascrizione	Fino a fine analisi	Cancellati dall'app; regola di scadenza 1 giorno
Log dell'applicazione e log di accesso HTTP	90 giorni, senza testo dei documenti, corpo delle richieste o token	Per scadenza
Log di sicurezza e amministrazione	12 mesi	Per scadenza
Copie di sicurezza (giornaliere, pre-rilascio, Irlanda)	14 giorni per ogni copia	Per rotazione
Copie del database prima delle migrazioni	Ultime 5, sullo stesso disco	A rotazione e nella cancellazione dello studio
Utenti	Finché attivi	Disattivazione immediata; cancellazione anche in Cognito con lo studio

11.1 **Alla cessazione del contratto**: 30 giorni di accesso in sola lettura con esportazione; cancellazione di tutti i dati dello studio entro i 30 giorni successivi, compresi testi estratti, cache OCR, conversazioni con gli agenti, indici, registri delle lavorazioni e utenti, con conferma scritta entro 5 giorni lavorativi dalla cancellazione (certificato di cancellazione, documento 54); uscita delle copie di sicurezza entro 14 giorni dalla cancellazione. In tutto, al massimo **74 giorni** dalla cessazione, salvo obblighi di legge.

11.2 **Restituzione.** Archivio ZIP cifrato con documenti originali, elaborati in DOCX e PDF/A, testi estratti in TXT, dati strutturati (anagrafiche, risposte dell'assessment, domande e fonti, versioni) in JSON e CSV, registro delle attività e log degli accessi penali in CSV, indice dei file con impronte SHA-256; consegna con link temporaneo cifrato o via API, entro 10 giorni lavorativi dalla richiesta, con estrazione assistita da Trailgun e certificato di restituzione (documento 53). L'esportazione complessiva in autonomia dall'app è la tappa R02 del Percorso. Assistenza all'uscita: 30 giorni inclusi; fino a 12 mesi per i clienti DORA o equiparati, alle condizioni economiche in vigore (piano di uscita, documento 56).

11.3 **Durante il contratto**, la cancellazione di una pratica toglie righe di documenti, controlli, versioni, comunicazioni, stati, firme, domande, attività, notifiche, conversazioni con gli agenti, la cache OCR dello studio e la cartella della pratica con originali, testi e indice; la cancellazione di un cliente fa lo stesso per tutte le sue pratiche. Le copie di sicurezza escono per rotazione in 14 giorni.

§ 12

Diritti degli interessati

Il Titolare risponde agli interessati; Trailgun gli dà gli strumenti (art. 28, par. 3, lett. e, GDPR). Procedura 27.

DIRITTO	COME LO ESERCITA IL TITOLARE SULLA PIATTAFORMA	STATO
Accesso (art. 15)	Ricerca nei documenti e nelle domande del fascicolo; scaricamento di documenti ed elaborati (DOCX, PDF/A, faldone); esportazione complessiva in formati aperti entro 10 giorni lavorativi.	IN ESSERE
Rettifica (art. 16)	Correzione degli elaborati e dei dati raccolti, con versione, autore e motivo. I documenti originali non si modificano: si sostituiscono o si cancellano.	IN ESSERE
Cancellazione (art. 17)	Cancellazione della pratica o del cliente, definitiva e completa (§ 11.3). Le copie di sicurezza escono per rotazione in 14 giorni.	IN ESSERE
Limitazione (art. 18)	Su istruzione del Titolare Trailgun sospende le lavorazioni della pratica; il Titolare può archiviarla.	SU ISTRUZIONE
Portabilità (art. 20)	Di rado applicabile ai dati delle pratiche; quando lo è, esportazione in JSON e CSV.	IN ESSERE
Opposizione (art. 21)	La valuta il Titolare; Trailgun esegue la cancellazione o la sospensione che ne deriva.	SU ISTRUZIONE
Decisioni automatizzate (art. 22)	Non ce ne sono: ogni elaborato è una bozza o una segnalazione che il professionista rivede.	IN ESSERE

12.1 Trailgun inoltra al Titolare entro **3 giorni lavorativi** le richieste che riceve direttamente dagli interessati e non vi risponde senza sua istruzione. Chi trova i propri dati nei documenti di un cliente viene indirizzato al cliente.

12.2 I diritti possono incontrare limiti di legge: l'art. 23 GDPR e l'art. 2-undecies, comma 1, lett. e), del Codice, quando dall'esercizio può derivare un pregiudizio effettivo e concreto alle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria. La valutazione è del Titolare.

12.3 Per i dati di cui Trailgun è titolare (utenti, fatturazione, contatti) si scrive a privacy@trailgun.ai; Trailgun risponde entro un mese, prorogabile nei casi dell'art. 12, par. 3, GDPR. Resta il diritto di reclamo al Garante.

§ 13

Violazioni dei dati personali

Che cosa succede quando qualcosa va storto, in che tempi, e che cosa resta al Titolare. Procedura 26; modelli di notifica 51.

MOMENTO	TRAILGUN VERSO IL TITOLARE	OBBLIGO DI LEGGE DEL TITOLARE
Conoscenza (T0)	Registrazione nel registro delle violazioni, triage, contenimento	–
Entro 2 ore	Al Titolare soggetto a DORA: notifica iniziale dell'incidente TIC, per email alla sua casella di sicurezza e per telefono al referente, con le informazioni disponibili	DORA: notifica iniziale all'autorità entro 4 ore dalla classificazione come grave e comunque entro 24 ore dalla conoscenza (Reg. delegato (UE) 2025/301, art. 5)
Entro 24 ore	A ogni Titolare: notifica della violazione dei dati personali, senza ingiustificato ritardo, con natura, categorie e numero approssimativo di interessati e registrazioni, conseguenze probabili, misure adottate o proposte, contatto (art. 33, par. 3)	Notifica al Garante entro 72 ore dalla conoscenza, se la violazione presenta un rischio (art. 33, par. 1)
Ogni 24 ore	Aggiornamenti fino alla chiusura e a ogni cambiamento rilevante; le informazioni mancanti si danno per fasi (art. 33, par. 4)	Comunicazione agli interessati se il rischio è elevato (art. 34)

MOMENTO	TRAILGUN VERSO IL TITOLARE	OBBLIGO DI LEGGE DEL TITOLARE
Entro 48 ore dalla notifica iniziale	Relazione intermedia sull'incidente TIC, con i dati per la classificazione e per i moduli di segnalazione (Reg. di esecuzione (UE) 2025/302)	DORA: relazione intermedia entro 72 ore dalla notifica iniziale
Entro 20 giorni dalla chiusura	Relazione finale sull'incidente TIC: cause, impatti, durata, dati coinvolti, azioni correttive	DORA: relazione finale entro un mese dall'ultima intermedia

13.1 Il responsabile informa il titolare «senza ingiustificato ritardo» (art. 33, par. 2, GDPR): la legge non fissa ore. Le 24 ore e i tempi DORA sono impegni contrattuali di Trailgun, più stretti di quelli del Titolare per lasciargli margine.

13.2 La notifica va al referente sicurezza e al DPO indicati nel Modulo d'ordine. Trailgun coopera nella valutazione, nelle notifiche e nel contenimento, documenta la violazione (art. 33, par. 5) e dà al Titolare un estratto del proprio registro delle violazioni su richiesta. Gli incidenti si classificano su tre livelli (grave, significativo, minore), allineati al Reg. delegato (UE) 2024/1772 (procedura 25).

13.3 **Rilevazione.** Una violazione si rileva con la sonda esterna e gli allarmi 24/7, GuardDuty, i log di accesso e di CloudTrail, le segnalazioni di utenti, fornitori e ricercatori a security@trailgun.ai. Per le violazioni di cui Trailgun è titolare (utenti, sito, fatturazione) la notifica al Garante entro 72 ore è di Trailgun.

13.4 Le minacce informatiche significative che possono riguardare il Titolare gli si comunicano entro 24 ore; l'assistenza in caso di incidente è senza costi aggiuntivi (art. 30, par. 2, lett. f, DORA).

V · §§ 14-19

Scelte di progetto e garanzie

Valutazione d'impatto, protezione fin dalla progettazione, personale, intelligenza artificiale, verifiche.

14 Valutazione d'impatto (DPIA)

14.1 La DPIA è del Titolare. È richiesta in particolare per il trattamento su larga scala di categorie particolari o di dati relativi a reati (art. 35, par. 3, lett. b, GDPR) e per le tipologie dell'elenco del Garante (art. 35, par. 4). Con dati dell'art. 10 e un sistema di intelligenza artificiale, due dei criteri delle linee guida EDPB sulla DPIA ricorrono quasi sempre: per molti clienti la DPIA è dovuta.

14.2 Trailgun assiste il Titolare (art. 28, par. 3, lett. f) fornendo entro **10 giorni lavorativi** le informazioni che gli servono, anche per la consultazione preventiva (art. 36). L'**Allegato 2** riassume descrizione, necessità e proporzionalità, diciassette rischi con misure e rischio residuo; il **documento 50** è lo stesso supporto in Word, con la descrizione già compilata e i campi del Titolare e del suo DPO.

15 Protezione fin dalla progettazione (art. 25)

15.1 **Le novità sono opzioni.** Ogni passo nuovo si accende e si spegne dalle impostazioni e dal modulo della singola pratica; spento, il flusso resta identico. La scelta si congela sulla pratica alla creazione. Trattative e revisione in Word sono spente per studio di default; la verifica giurisprudenziale è spenta di default; l'OCR di riserva fuori dall'UE è spento di default.

15.2 **Niente dati inventati, niente fonti esterne.** Ogni dato dell'elaborato viene dai documenti, con la fonte, o è «N/D»; il raccoglitore dati non consulta fonti esterne.

15.3 **Regime dei fascicoli penali.** Sui fascicoli penali o misti niente embeddings e registro degli accessi. La materia la sceglie l'avvocato prima di caricare; senza scelta la ricava un classificatore. Il filtro per imputato e la scheda dell'imputato mostrano solo ciò che riguarda una persona, e ogni loro consultazione è registrata.

15.4 **Accesso minimo.** Login solo su invito, TOTP per tutti, visibilità per cliente, ruoli con permessi concessi uno a uno, ruolo di sola lettura, chiavi API conservate come impronta.

15.5 **Nessun tracciamento.** Il sito non usa cookie né strumenti di analisi o profilazione e non carica risorse esterne; l'app usa solo la sessione di autenticazione.

15.6 **Costi senza contenuti.** Ogni chiamata ai modelli registra modello, agente, quantità e costo, mai il testo.

15.7 **Dati nell'Unione per costruzione.** Il codice rifiuta una regione dei modelli fuori dall'UE; gli embeddings accettano solo un modello nell'UE; le ricerche giuridiche e le notifiche esterne escono senza dati delle pratiche; la cache OCR non attraversa i confini dello studio.

16 Personale, riservatezza e segreto professionale

16.1 Trailgun autorizza solo chi ne ha bisogno per il proprio compito, lo designa per iscritto (art. 29 GDPR e art. 2-quaterdecies del Codice) e lo vincola alla riservatezza, anche dopo la fine del rapporto.

16.2 I dati delle pratiche possono essere coperti dal segreto professionale dell'avvocato o dal segreto bancario. L'avvocato deve far rispettare il segreto anche a consulenti e collaboratori (art. 28 del Codice deontologico forense): Trailgun ne tiene conto e tratta questi dati con il medesimo rigore.

16.3 L'accesso tecnico alla produzione è concentrato nel CEO. Lo bilanciano credenziali solo temporanee con secondo fattore, CloudTrail e sessioni registrate per 12 mesi, il registro degli accessi del personale ai contenuti, la revisione trimestrale degli accessi e un runbook di ripristino scritto e provato; il deposito del codice presso un terzo è la tappa R09 del Percorso.

17 Intelligenza artificiale e dati personali

17.1 **Addestramento.** Né Trailgun né chi esegue i modelli usa i dati delle pratiche, i documenti o gli elaborati per addestrare, ottimizzare o valutare modelli IN ESSERE. Su Amazon Bedrock i dati restano nella regione e il produttore del modello non li riceve; la dichiarazione firmata è il documento 60.

17.2 **Nessuna decisione automatizzata.** Gli agenti preparano bozze, analisi e segnalazioni con le fonti; un professionista del Titolare le rivede prima dell'uso. Non c'è profilazione.

17.3 **Cache del prompt.** Nell'analisi estesa il fascicolo resta nella cache del prompt di Bedrock, nella stessa regione, per un'ora, per non rileggerlo a ogni domanda.

17.4 **Trasparenza.** Marcatura leggibile da macchina «AI-generated, EU AI Act art. 50» nei metadati dei DOCX e PDF prodotti dagli agenti; avviso di IA nelle chat, sulla pagina dell'atto e nelle mail inviate in modalità automatica (art. 50, par. 1 e 2, Reg. (UE) 2024/1689) IN ESSERE. Il documento 09 riporta la scheda di trasparenza del sistema; il documento 19 è il modello di informativa dello studio ai propri clienti.

17.5 Il Parere EDPB 28/2024 sui modelli di IA riguarda soprattutto chi sviluppa e addestra modelli; Trailgun li usa senza addestrarli sui dati dei clienti.

18 Verifiche, documenti e certificazioni

18.1 Verifiche del Titolare: una all'anno con 30 giorni di preavviso, in orario lavorativo, fino a 2 giorni in loco; straordinarie dopo un incidente grave o su richiesta di un'autorità, con 5 giorni lavorativi di preavviso; illimitate per le funzioni DORA essenziali o importanti e per le autorità (art. 30, par. 3, lett. e, DORA; art. 8 d.lgs. 10 marzo 2025, n. 23). Questionari: risposta entro 15 giorni lavorativi, uno all'anno senza costi. Modulo di richiesta: documento 52.

18.2 Su richiesta e sotto riservatezza: questo documento, il registro dei trattamenti (documento 40) per la parte del Titolare, il supporto alla DPIA (documento 50), l'elenco dei fornitori a valle, le valutazioni dei trasferimenti, i verbali delle prove di ripristino, l'estratto del registro delle violazioni, i rapporti di AWS da AWS Artifact.

18.3 L'infrastruttura è certificata da AWS (ISO/IEC 27001, 27017, 27018, SOC 2, C5). Il percorso di Trailgun è nel documento 12: primo penetration test indipendente (R06), gap assessment ISO/IEC 27001:2022 (R07), sistema di gestione definitivo (R08), stage 1 (R15), certificato (R16); la valutazione di ISO/IEC 42001 (R17) è un obiettivo.

19 Assicurazioni

19.1 Polizza cyber e polizza di responsabilità civile professionale per errori e omissioni del software, per [€ ...] per sinistro e per anno, con [compagnia] IN ESSERE; certificato su richiesta.

§ 20

Garanzie in essere

Le garanzie che toccano i dati personali, con l'evidenza che Trailgun mostra in sede di audit. Le tappe successive (certificazioni, nuova piattaforma) sono nel documento 12, con le loro date.

#	GARANZIA	EVIDENZA
1	Tutti gli agenti su Claude in Amazon Bedrock nelle regioni UE; nessun gateway esterno né fornitore di modelli diretto	Configurazione di produzione; codice che rifiuta le regioni fuori dall'UE, con test
2	Embeddings solo su Bedrock nell'UE (Amazon Titan), mai sui fascicoli penali; indici precedenti rigenerati	Configurazione; codice dell'indice
3	Opt-out dei servizi di IA di AWS (Textract, Transcribe, Bedrock); account AWS dedicato e intestato a Trailgun	Policy di AWS Organizations; intestazione dell'account
4	OCR di riserva DocuPipe come opzione dello studio, spenta di default	Impostazione predefinita
5	Notifiche esterne senza dati delle pratiche	Esempio di notifica; codice
6	Log di accesso HTTP e applicativi 90 giorni, senza testo dei documenti, corpo delle richieste o token	Gruppi di log e loro conservazione
7	HSTS e intestazioni di sicurezza	Intestazioni delle risposte
8	Copie pre-rilascio con scadenza a 14 giorni; tutte le copie escono in 14 giorni	Elenco degli snapshot e loro scadenze
9	Cancellazione completa: cache OCR per studio e cancellata con la pratica, conversazioni con gli agenti, eventi di costo scollegati dai contenuti, archivio One LEGALE, copie del database; strumento di cancellazione di studio e utenti a fine contratto	Codice e test; verbale della prova di cancellazione; certificato 54
10	CloudTrail su tutte le regioni con convalida dell'integrità, 12 mesi; GuardDuty; sessioni SSM registrate; MFA su tutte le console	Configurazione; revisione degli accessi (modello 44)
11	Sonda esterna ogni minuto e allarmi 24/7	Allarmi configurati; prova di un allarme
12	Ricerche verso One LEGALE senza nomi, codici fiscali, importi e dati delle pratiche	Regola in codice e test
13	Prova di ripristino trimestrale con RTO misurato; prova automatica nella CI	Verbale della prova del `[data]`; esiti della CI
14	Marcatura «AI-generated» in DOCX e PDF; avviso di IA nelle chat, sulla pagina dell'atto e nelle mail automatiche	File di esempio; schermate
15	Ruoli operator e viewer imposti dal server	Codice e test dei ruoli
16	Credenziali amministrative solo temporanee (IAM Identity Center); 2FA obbligatoria nell'organizzazione GitHub	Configurazione
17	Caselle security@ e privacy@ presidiate; DPO nominato e comunicato al Garante	Lettera di nomina; ricevuta della comunicazione
18	DPA firmati con AWS, Resend, DocuPipe, Openapi, Wolters Kluwer; valutazioni dei trasferimenti verso Resend e DocuPipe	Contratti archiviati; valutazioni
19	Registro delle violazioni e procedura con classificazione su tre livelli	Procedure 25 e 26; registro
20	Registro degli accessi del personale al contenuto delle pratiche	Registro; estratto al Titolare
21	Container dell'app non root; immagine del proxy fissata a una versione	Configurazione dell'immagine
22	Polizze cyber e RC professionale in essere	Certificati assicurativi

ALLEGATO 1 · PARTE A

Registro delle categorie di attività di trattamento svolte per conto dei Titolari

Art. 30, par. 2, GDPR, in sintesi. Il registro completo, per modulo, con i sub-responsabili, i trasferimenti e le misure, è il foglio di calcolo del documento 40. Trailgun tiene il registro anche se ha meno di 250 dipendenti, perché il trattamento non è occasionale e comprende dati degli artt. 9 e 10 (art. 30, par. 5). L'elenco nominativo dei Titolari è tenuto a parte ed è estratto, per la sua riga, al Titolare che lo chiede.

VOCE (ART. 30, PAR. 2)	CONTENUTO
a) Responsabile	[Trailgun S.r.l.], [sede], C.F. e P.IVA [...], PEC [...]; legale rappresentante Franco Puppo, CEO; privacy@trailgun.ai
a) Titolari per conto dei quali agisce	Ogni cliente con contratto e DPA in vigore, con nome, contatti, referente sicurezza e DPO dal Modulo d'ordine; per le catene, anche il titolare a monte indicato dal cliente (DPA, art. 2.4)
a) DPO	[DPO esterno: nome o società], dpo@[...]
b) Categorie di trattamenti	Tabella seguente, R-01 … R-15
c) Trasferimenti	§ 9: Resend (Data Privacy Framework e clausole tipo), DocuPipe solo per chi lo attiva (clausole tipo), canali di notifica senza dati delle pratiche
d) Misure di sicurezza	§ 10 di questo documento, Allegato 2 del DPA, documento 05

ID	CATEGORIA DI TRATTAMENTO	OPERAZIONI	INTERESSATI E DATI	SUB-RESPONSABILI	FUORI UE
R-01	Ricezione e conservazione dei documenti	Caricamento dal modulo, lotti, caselle email, API; conservazione su disco cifrato	Tutti quelli del § 4	AWS; Resend per le caselle	Resend (società USA)
R-02	Estrazione del testo e OCR	Lettura locale di Word ed Excel; OCR con coordinate, segmentazione dei PDF con più atti; cache del testo per studio	Tutti quelli del § 4	AWS (Textract); DocuPipe se lo studio lo accende	DocuPipe, solo se acceso
R-03	Trascrizione audio	Trascrizione con distinzione dei parlanti	Persone registrate o intercettate; voce, contenuto delle conversazioni	AWS (Transcribe)	No
R-04	Elaborazione con agenti di IA	Classificazione, analisi, raccolta dei dati con fonte, redazione, controllo, domande, funzioni sul fascicolo, assistente dell'atto	Tutti quelli del § 4	AWS (Bedrock, regioni UE)	No
R-05	Indicizzazione e ricerca	Embeddings dei passaggi (Amazon Titan) e ricerca lessicale locale; mai embeddings sul penale	Dati nei passaggi dei documenti	AWS (Bedrock, regioni UE)	No
R-06	Ricerca di fonti giuridiche	Ricerche composte dal modello su One LEGALE, senza dati delle pratiche	Nessun dato delle pratiche	Wolters Kluwer Italia	No
R-07	Comunicazioni con i clienti del Titolare e trattative	Invio di richieste e messaggi, ricezione di risposte e allegati	Clienti del Titolare, controparti, notaio; contatti, testi, allegati	Resend	Resend (società USA)
R-08	Notifiche agli utenti	Avvisi in app; email, Telegram, SMS e WhatsApp con solo avviso e link	Utenti; avviso generico	Resend, Telegram, Twilio	Telegram, Twilio, senza dati delle pratiche

ID	CATEGORIA DI TRATTAMENTO	OPERAZIONI	INTERESSATI E DATI	SUB-RESPONSABILI	FUORI UE
R-09	Firma digitale e visure	Firma qualificata dei PDF; visure camerali	Firmatari; imprese e loro esponenti	Openapi, Namirial	No
R-10	Revisione in Word e conversione	Ricezione della versione rivista, conversione in PDF/A sul server, marcatura dei metadati	Dati nell'atto	AWS	No
R-11	Assistenza	Agente di supporto, ticket e allegati	Utenti; dati delle pratiche eventualmente riportati	AWS (Bedrock, regioni UE)	No
R-12	Memoria dello studio	Registrazione delle regole confermate dagli utenti	Eventuali dati nelle regole	AWS	No
R-13	Copie di sicurezza e ripristino	Snapshot giornalieri e pre-rilascio, copie in Irlanda, prove di ripristino, ripristino	Tutti	AWS	No
R-14	Esportazione, restituzione, cancellazione	Scaricamenti, esportazione complessiva, cancellazione di pratiche, clienti, studi e utenti	Tutti	AWS	No
R-15	Registri per il Titolare	Registro delle attività di studio, log degli accessi ai fascicoli penali, registro degli accessi del personale	Utenti; riferimenti a clienti e pratiche	AWS	No

ALLEGATO 1 · PARTE B

Trattamenti di cui Trailgun è titolare

Art. 30, par. 1, GDPR, in sintesi. Titolare: [Trailgun S.r.l.]; DPO come sopra.

TRATTAMENTO	FINALITÀ E BASE	INTERESSATI E DATI	DESTINATARI	FUORI UE	CONSERVAZIONE
Account e autenticazione	Fornire e proteggere il servizio; art. 6.1.f e b	Utenti: email, ruolo, studio, preferenze, attività, chat Telegram	AWS (Cognito, SES)	No	Durata del contratto, poi come i dati dello studio (§ 11.1)
Sicurezza e registri tecnici	Sicurezza della piattaforma; art. 6.1.f	Utenti e visitatori: IP, data e ora, richiesta, browser	AWS (CloudWatch, CloudTrail)	No	90 giorni (accessi e applicazione); sicurezza 12 mesi
Assistenza	Prestare l'assistenza prevista; art. 6.1.b	Utenti: conversazioni, ticket	AWS (Bedrock, regioni UE)	No	Durata del contratto, poi come i dati dello studio
Fatturazione e contratto	Obblighi fiscali e contrattuali; art. 6.1.c e b	Referenti dello studio: dati fiscali; carta tramite Stripe	Stripe, consulenti fiscali [...]	Stripe	10 anni (art. 2220 c.c.)
Contatti commerciali	Rispondere e presentare il servizio; art. 6.1.b e f; promozioni solo con consenso	Referenti di banche, intermediari e studi: nome, contatti, messaggi	Google (Workspace)	Garanzie di Google	Il tempo necessario alla richiesta; se nasce un rapporto, la sua durata
Sito trailgun.ai	Funzionamento e protezione del sito; art. 6.1.f	Visitatori: dati tecnici delle richieste; nessun cookie	AWS	No	Come i registri tecnici
Segnalazioni	Segnalazioni di vulnerabilità e whistleblowing; art. 6.1.c e f	Segnalanti e persone citate	Google (Workspace)	Garanzie di Google	Il tempo necessario alla gestione (politica P17)

ALLEGATO 2

Supporto alla valutazione d'impatto del Titolare

Art. 35, par. 7, GDPR: descrizione sistematica (lett. a), necessità e proporzionalità (lett. b), rischi (lett. c), misure (lett. d). È precompilato da Trailgun con ciò che sa della piattaforma; il Titolare lo completa con il proprio contesto e ne decide l'esito. La versione compilabile in Word, con i campi per l'esito e il parere del DPO, è il documento 50.

A.1 Descrizione sistematica

a **Natura.** Trattamento automatizzato, continuativo, dei documenti delle pratiche con agenti di intelligenza artificiale che leggono, estraggono, analizzano e redigono; revisione umana di ogni elaborato da parte di un professionista del Titolare; nessuna decisione automatizzata.

b **Ambito.** Interessati e categorie del § 4, compresi dati dell'art. 10 e, occasionalmente, dell'art. 9; volume variabile, fino a migliaia di debitori per un data tape o un lotto; conservazione decisa dal Titolare durante il contratto, al massimo 74 giorni dopo la cessazione (§ 11).

c **Contesto.** Interessati che non hanno rapporti con Trailgun e di solito non sanno del trattamento; dati spesso coperti da segreto professionale o bancario; uso di una tecnologia nuova (modelli linguistici); fornitore giovane, con l'accesso tecnico concentrato in una persona e bilanciato dai controlli del § 16.3.

d **Finalità.** Quelle del Titolare: difesa in giudizio, recupero e gestione dei crediti, due diligence, cartolarizzazioni, procedure concorsuali, escussione di garanzie, trattative.

e **Flussi, luoghi e fornitori.** §§ 6-9; registro nell'Allegato 1 e nel documento 40.

A.2 Criteri che fanno ritenere necessaria la DPIA

- [x] Dati relativi a reati o categorie particolari — artt. 9 e 10 GDPR; art. 35, par. 3, lett. b)
- [ ] Larga scala — da valutare: data tape, lotti, fascicoli penali estesi
- [ ] Combinazione di insiemi di dati — solo dentro la pratica: nessuna fonte esterna
- [ ] Monitoraggio sistematico — no
- [x] Uso innovativo di tecnologie — modelli linguistici di grandi dimensioni
- [ ] Interessati vulnerabili — da valutare: debitori in difficoltà, minori citati
- [ ] Valutazione o punteggio di persone — no: si valutano documenti e crediti, non il merito creditizio
- [ ] Decisioni automatizzate con effetti giuridici — no: art. 22 non applicabile

A.3 Necessità e proporzionalità

- **Finalità determinate e legittime**: quelle del Titolare, con le basi del § 5; Trailgun non tratta per finalità proprie.
- **Minimizzazione**: si trattano solo i documenti che il Titolare carica, per la lavorazione che avvia; nessun arricchimento esterno; sui fascicoli penali niente embeddings; ricerche giuridiche e notifiche senza dati delle pratiche; il Titolare evita di caricare categorie particolari non necessarie e usa titoli neutri per le pratiche.
- **Esattezza**: ogni dato dell'elaborato ha la fonte o è «N/D»; il professionista rivede tutto.
- **Limitazione della conservazione**: cancellazione completa per pratica e per cliente in ogni momento; tempi alla cessazione del § 11.
- **Informazione**: del Titolare, con le eccezioni dell'art. 14, par. 5, lett. b) e d); informazione ai clienti sull'uso dell'IA (art. 13 della legge 132/2025, modello 19).
- **Diritti**: strumenti del § 12; inoltro in 3 giorni lavorativi.
- **Responsabili e trasferimenti**: DPA ai sensi dell'art. 28; fornitori del § 8; trasferimenti del § 9, limitati a servizi accessori con le loro garanzie.
- **Alternativa meno invasiva**: il lavoro manuale sugli stessi documenti; l'uso del sistema la sostituisce con un trattamento più tracciato (fonti, versioni, registro degli accessi).

A.4

Rischi per i diritti e le libertà, misure e rischio residuo

Valutazione proposta da Trailgun: probabilità e gravità combinate in basso, medio, alto, sulle misure in essere al 01/12/2026. Dove una tappa del Percorso riduce ancora il rischio, la colonna finale ne riporta il codice.

ID	RISCHIO	INIZIALE	MISURE IN ESSERE	RESIDUO	PERCORSO
R1	Un utente di uno studio vede dati di un altro studio per un errore di isolamento	Alto	Predicato unico di visibilità con test a ogni rilascio; cache OCR per studio	Basso	–
R2	Accesso con credenziali di un utente rubate	Alto	Invito, TOTP obbligatorio, verifica del token su ogni richiesta, disattivazione immediata	Basso	–
R3	Abuso o compromissione dell'accesso amministrativo	Alto	Niente SSH; SSM con sessioni registrate; credenziali temporanee con MFA; CloudTrail 12 mesi; registro degli accessi ai contenuti; revisione trimestrale	Medio	R13
R4	Dati delle pratiche fuori dall'UE presso fornitori dei modelli	Alto	Modelli ed embeddings su Bedrock nelle regioni UE; regioni fuori dall'UE rifiutate dal codice	Basso	–
R5	Accesso di autorità di paesi terzi presso fornitori con capogruppo statunitense	Medio	Regioni UE, cifratura, contestazione delle richieste (art. 48 GDPR), informazione al Titolare	Medio	R12
R6	Riuso dei dati per addestrare modelli	Alto	Nessun addestramento da parte di Trailgun; Bedrock senza condivisione con il produttore del modello; opt-out dei servizi di IA di AWS	Basso	–
R7	Divulgazione tramite notifiche esterne	Medio	Solo avviso generico e link; canali esterni scelti dall'utente	Basso	–
R8	Divulgazione tramite le ricerche verso la banca dati giuridica	Medio	Regola e test che tolgono nomi e dati; verifica giurisprudenziale spenta di default	Basso	–
R9	Perdita di disponibilità o di integrità	Alto	Snapshot giornaliero e copia in Irlanda; prova di ripristino trimestrale e nella CI; sonda e allarmi 24/7	Medio	R01, R03, R12
R10	Conservazione oltre il necessario	Alto	Copie con scadenza a 14 giorni; cancellazione completa con strumento e certificato	Basso	–
R11	Elaborato inesatto che danneggia un interessato (per esempio un importo errato)	Alto	Fonte per ogni dato o «N/D», agenti di controllo, calcoli in codice, revisione del professionista	Medio	dipende dalla revisione del Titolare
R12	Trattamento eccessivo di dati di terzi estranei nei fascicoli penali e nelle intercettazioni	Alto	Niente embeddings, registro degli accessi, filtro per imputato; minimizzazione del Titolare	Medio	dipende dal Titolare
R13	Diritti non soddisfatti per cancellazione o esportazione incompleta	Medio	Cancellazione completa; esportazione complessiva assistita in 10 giorni lavorativi	Basso	R02
R14	Violazione non rilevata o notificata in ritardo	Alto	Notifica in 24 ore; log di accesso; sonda, allarmi, CloudTrail e GuardDuty; procedura 26	Basso	R05, R06
R15	File malevolo caricato che compromette la piattaforma	Medio	Limiti sugli archivi, apertura nel container senza privilegi, componenti aggiornati, scansione delle immagini	Medio	R06, R12
R16	Errore di configurazione del Titolare (visibilità, utenti)	Medio	Visibilità per cliente, ruoli, registro delle attività; misure del Titolare (DPA, art. 6.4)	Medio	dipende dal Titolare
R17	File inviati negli Stati Uniti dall'OCR di riserva	Medio	Opzione per studio spenta di default; clausole tipo e valutazione del trasferimento	Basso	–

A.5 Come si legge e che cosa resta al Titolare

Con le misure in essere nessun rischio resta alto. I rischi R11, R12 e R16 dipendono anche dalle misure del Titolare: revisione degli elaborati, minimizzazione dei dati caricati, gestione degli utenti e della visibilità. I rischi medi R3, R5, R9 e R15 si riducono ancora con le tappe del Percorso indicate. Se il rischio residuo resta alto per il contesto del Titolare, questi consulta il Garante prima del trattamento (art. 36 GDPR); Trailgun lo assiste.

A.6 Esito della valutazione

L'esito, le misure aggiuntive del Titolare e il parere del suo DPO si registrano nel modello compilabile del documento 50, Supporto alla valutazione d'impatto (DPIA) del Titolare, che riporta la versione di questo documento su cui si fonda la valutazione (2.0, 01/12/2026) e la data del prossimo riesame.

ENGLISH SUMMARY · STATUS AS OF 1 DECEMBER 2026

Data protection, step by step

A courtesy summary for international banks and their DPOs. The Italian text prevails. Every measure described is in place, with evidence available for audit; future milestones are dated in document 12.

- **Roles.** For case data the client (bank, financial intermediary, servicer or law firm) is the controller and Trailgun the processor under Art. 28 GDPR, or a sub-processor when the client itself acts for another controller, such as a servicer for a securitisation vehicle. Trailgun is a controller only for user accounts, platform security, support, billing and sales contacts.
- **Data.** Case documents with financial data, criminal-law data (Art. 10 GDPR, Art. 2-octies Italian Privacy Code), occasional special categories (Art. 9), audio recordings and intercepted communications. No profiling, no automated decisions (Art. 22).
- **Location.** Data at rest in Frankfurt (AWS eu-central-1); encrypted backup copies in Ireland (eu-west-1). All models (Anthropic Claude) and embeddings (Amazon Titan) run on Amazon Bedrock in EU regions; non-EU regions are refused by code. The model maker does not receive the data.
- **Other non-EU flows.** Resend (US company, sending from Ireland; EU-US Data Privacy Framework, transfer impact assessment done); DocuPipe (US) fallback OCR only for firms that switch it on, off by default; Telegram, SMS and WhatsApp notifications carry no case data.
- **Training.** Neither Trailgun nor the model provider trains on client data; AWS AI services opt-out policy in AWS Organizations.
- **Security.** Encrypted volumes (AES-256, AWS KMS), TLS with HSTS, mandatory TOTP MFA for all users, invitation-only access, per-firm logical isolation through a single tested visibility check, per-firm OCR cache, hashed API keys, no SSH, temporary admin credentials, CloudTrail and GuardDuty, external probe with 24/7 alerts, secret scanning and a restore drill before every release.
- **Breaches.** Notice to the controller within 24 hours; for DORA clients also an initial ICT incident notice within 2 hours, updates every 24 hours, an intermediate report within 48 hours and a final report within 20 days of closure.
- **Sub-processors.** Published at https://trailgun.ai/subprocessors; 30 days' prior notice, 60 for DORA critical or important functions, right to object and to terminate without penalty.
- **Retention and exit.** Kept until the client deletes; deletion is complete (OCR cache and agent conversations included). After termination: 30 days read-only with export, deletion within the next 30 days with a written certificate, backups rotated out within 14 more days (74 days at most).
- **Rights, DPIA, audits.** Data subject requests forwarded within 3 working days; DPIA information within 10 working days, with a pre-filled DPIA annex and an editable template (document 50); one audit a year on 30 days' notice, unlimited for DORA critical functions and authorities.

Contacts and documents. Legal representative: Franco Puppo, CEO. Privacy: privacy@trailgun.ai; security and breaches: security@trailgun.ai. DPO: [name or firm] . The processor's record of processing (Art. 30(2) GDPR) is summarised in Annex 1 and kept in full in document 40; the DPIA support (Art. 35(7)) is Annex 2 and document 50; the binding terms are in the Data Processing Agreement (document 07).

Trailgun

On target.

In a flash.

Dai documenti al lavoro finito: agenti AI per pratiche legali e finanziarie.

PRIVACY	SICUREZZA E VIOLAZIONI	DPO	SITO
privacy@trailgun.ai	security@trailgun.ai	[nome o società]	trailgun.ai

Documenti collegati: 07 Accordo sul trattamento dei dati · 40 Registro dei trattamenti del responsabile · 50 Supporto alla DPIA · 15 Registro dei subfornitori. L'indice completo del pacchetto di conformità è nel Trust Center (documento 00).