Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO 07

VERSIONE 2.0 · DICEMBRE 2026

Accordo sul trattamento dei dati personali

Atto di designazione del Responsabile del trattamento ai sensi dell'art. 28 del Regolamento (UE) 2016/679, per studi legali, banche, intermediari e servicer, con i quattro allegati: descrizione del trattamento, misure di sicurezza, sub-responsabili, trasferimenti.

TITOLARE	RESPONSABILE	ORIGINE DEI DATI	DATI A RIPOSO
Studio, banca o servicer	Trailgun, art. 28 GDPR	Solo dal Titolare	Unione europea

ACCORDO SUL TRATTAMENTO DEI DATI PERSONALI

Atto di designazione del Responsabile del trattamento ai sensi dell'art. 28 GDPR

Le parti evidenziate [così] si completano prima della firma. Gli articoli segnati 1341 richiedono l'approvazione specifica del Titolare ai sensi degli artt. 1341 e 1342 c.c. e sono riepilogati nella pagina delle firme. Le misure descritte negli Allegati sono in essere alla sottoscrizione; le tappe successive sono vincolanti per rinvio al Percorso di certificazione e piattaforma (documento 12, art. 21.5).

TRA

TITOLARE DEL TRATTAMENTO

[Studio legale, banca, intermediario o servicer]

con sede in [indirizzo], C.F. / P.IVA [...], iscritto all'Ordine degli Avvocati di [...] o all'albo o elenco di vigilanza [...], LEI [...] se entità finanziaria, in persona di [legale rappresentante], PEC [...]; DPO, se nominato: [...]

(il «**Titolare**»)

RESPONSABILE DEL TRATTAMENTO

[Trailgun S.r.l.]

con sede in [indirizzo], C.F. e P.IVA [...], iscritta al Registro delle imprese di [...], REA [...], LEI [...], in persona di **Franco Puppo**, CEO e legale rappresentante, PEC [...]; referente privacy privacy@trailgun.ai; DPO [...]

(«**Trailgun**» o il «**Responsabile**»)

PREMESSO CHE

A. Il Titolare esercita la professione forense, oppure un'attività bancaria o finanziaria, compresa la gestione, il recupero, l'acquisto o la cartolarizzazione di crediti, e nello svolgerla tratta dati personali dei propri clienti, dei debitori, delle controparti e dei terzi coinvolti, determinandone finalità e mezzi: è quindi titolare del trattamento ai sensi dell'art. 4, n. 7, GDPR, salvo il caso dell'art. 2.4.

B. Trailgun gestisce la piattaforma Trailgun, con cui agenti di intelligenza artificiale leggono i documenti di una pratica e ne ricavano atti, analisi e verifiche che un professionista rivede (il «Servizio»), in forza del contratto di servizio stipulato tra le parti (il «Contratto»).

C. Per erogare il Servizio Trailgun riceve dal Titolare i documenti delle pratiche e i dati personali che contengono. Non li raccoglie presso gli interessati, non li sceglie e non ne decide l'uso: li acquisisce dal Titolare, che ne resta titolare, e li tratta esclusivamente per suo conto e secondo le sue istruzioni.

D. L'art. 28 GDPR impone che il trattamento affidato a un responsabile sia disciplinato da un contratto che vincoli il responsabile al titolare e ne stabilisca materia, durata, natura, finalità, tipo di dati, categorie di interessati, obblighi e diritti delle parti.

E. Trailgun dichiara di presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, descritte nell'Allegato 2, in modo che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti degli interessati, e ha descritto al Titolare la piattaforma, i suoi fornitori e le tappe successive del proprio percorso di certificazione.

F. Le parti tengono conto del d.lgs. 30 giugno 2003, n. 196 come modificato (il «Codice»), delle Linee guida EDPB 07/2020 sui concetti di titolare e responsabile, del Parere EDPB 22/2024 sulla catena dei sub-responsabili, del Regolamento (UE) 2024/1689 sull'intelligenza artificiale, della legge 23 settembre 2025, n. 132 e, per il Titolare soggetto a DORA, del Regolamento (UE) 2022/2554, del Regolamento delegato (UE) 2025/532 e del d.lgs. 10 marzo 2025, n. 23.

Tutto ciò premesso, le parti convengono quanto segue. Le premesse e gli allegati fanno parte integrante dell'accordo.

ARTICOLI

Accordo sul trattamento dei dati personali

Ai sensi dell'art. 28 del Regolamento (UE) 2016/679 («GDPR»). Si sottoscrive insieme al Modulo d'ordine del Contratto, o da solo; per i dati personali prevale sugli altri documenti contrattuali, salvo l'Allegato DORA (documento 18, art. 21.2).

IN BREVE

- Il cliente è il titolare dei dati delle pratiche; Trailgun è il suo responsabile del trattamento, o il suo sub-responsabile se il cliente tratta per conto di altri.
- Trailgun riceve i dati solo dal Titolare, li tratta solo su sua istruzione e solo per il Servizio.
- Nessun addestramento di modelli, né da parte di Trailgun né di chi esegue i modelli; nessun riuso tra clienti; nessun contatto con gli interessati che il Titolare non abbia attivato.
- Dati a riposo nell'Unione europea; modelli ed embeddings su Amazon Bedrock nelle regioni dell'Unione.
- Violazioni notificate entro 24 ore; sub-responsabili annunciati 30 giorni prima, 60 per le funzioni DORA essenziali o importanti.
- A fine contratto i dati tornano al Titolare e si cancellano, copie comprese, entro 74 giorni, con conferma scritta.

Art. 1 Definizioni

1.1 I termini «dati personali», «trattamento», «interessato», «titolare», «responsabile», «violazione dei dati personali», «categorie particolari di dati» e gli altri termini del GDPR hanno il significato dell'art. 4 GDPR.

1.2 Nell'accordo si intendono per: **Dati delle Pratiche**, i dati personali contenuti nei documenti, nei messaggi, nelle registrazioni audio e negli altri contenuti che il Titolare affida a Trailgun, e negli Elaborati; **Elaborati**, gli atti, le analisi, le relazioni, le risposte, le timeline, le schede e ogni altro risultato prodotto dalla Piattaforma; **Piattaforma**, l'applicazione Trailgun (app.trailgun.ai) e le sue interfacce di programmazione; **Utenti**, gli avvocati, i praticanti, i collaboratori e i dipendenti che il Titolare abilita alla Piattaforma; **Sub-responsabile**, il fornitore di cui Trailgun si avvale per specifiche attività di trattamento per conto del Titolare; **Titolare soggetto a DORA**, l'entità finanziaria soggetta al Regolamento (UE) 2022/2554 o l'intermediario dell'art. 106 TUB cui le sue norme si applicano per l'art. 6 del d.lgs. 10 marzo 2025, n. 23, che lo ha indicato nel Modulo d'ordine.

1.3 Gli altri termini con l'iniziale maiuscola hanno il significato delle Condizioni generali di servizio.

Art. 2 Designazione e ruoli delle parti

2.1 Il Titolare designa Trailgun responsabile del trattamento dei Dati delle Pratiche ai sensi dell'art. 28 GDPR. Trailgun accetta la designazione e si obbliga a trattare i dati nel rispetto del GDPR, del Codice e di questo accordo.

2.2 Il Titolare tratta i Dati delle Pratiche per le proprie finalità: per lo studio legale, assistenza e consulenza ai clienti, attività stragiudiziale e difesa in giudizio; per la banca, l'intermediario e il servicer, gestione e recupero dei crediti, due diligence, cartolarizzazioni, procedure concorsuali ed escussione di garanzie. Determina finalità e mezzi essenziali del trattamento: quali pratiche e quali documenti affidare a Trailgun, quali lavorazioni avviare, chi tra i suoi Utenti vi accede, quando cancellare. Risponde verso gli interessati della liceità del trattamento.

2.3 Trailgun non determina finalità né mezzi essenziali. Le scelte tecniche e organizzative non essenziali (infrastruttura, modelli, misure di sicurezza, fornitori) spettano a Trailgun nei limiti di questo accordo, come ammesso dalle Linee guida EDPB 07/2020.

2.4 Se il Titolare tratta i dati a sua volta per conto di un terzo, come il servicer per conto di una società veicolo di cartolarizzazione o di una banca, lo indica nelle condizioni particolari del Modulo d'ordine: per quell'incarico Trailgun è sub-responsabile, gli obblighi di questo accordo valgono verso il Titolare e il Titolare garantisce di aver ottenuto dal proprio titolare l'autorizzazione a ricorrere a Trailgun e ai sub-responsabili dell'Allegato 3. Trailgun gli fornisce le informazioni necessarie a documentare la catena.

2.5 Questo accordo non riguarda i trattamenti per cui Trailgun è titolare autonomo: gli account degli Utenti, la sicurezza della Piattaforma, la gestione dell'assistenza, la fatturazione, l'amministrazione del Contratto e i contatti commerciali, descritti nell'informativa privacy di Trailgun e nel documento 06, Protezione dei dati personali (§ 3.4).

Art. 3 Acquisizione dei dati: solo dal Titolare

3.1 Trailgun acquisisce i Dati delle Pratiche esclusivamente dal Titolare e dai suoi Utenti, attraverso i canali che il Titolare sceglie: (a) il caricamento nella Piattaforma; (b) l'invio di più pratiche in un unico archivio; (c) le caselle email dedicate dello studio, alle quali il Titolare, o chi da lui indicato, inoltra documenti; (d) l'interfaccia di programmazione, con chiavi rilasciate al Titolare.

3.2 Trailgun non raccoglie dati presso gli interessati, non li cerca né li integra con fonti esterne di propria iniziativa e non ha rapporti diretti con gli interessati. Si considerano acquisiti per conto e su istruzione del Titolare, e restano Dati delle Pratiche, soltanto: (a) le risposte che i clienti del Titolare inviano alle richieste di documenti o informazioni che il Titolare attiva sulla pratica; (b) i risultati delle interrogazioni di registri pubblici, come le visure camerali, che il Titolare richiede per la singola pratica; (c) i messaggi delle controparti e degli altri partecipanti alle trattative che il Titolare attiva, ricevuti agli indirizzi dedicati di quella trattativa.

3.3 Le email che arrivano alle caselle dedicate da mittenti non ammessi non aprono pratiche. I documenti che arrivano da mittenti non riconosciuti in risposta alle richieste restano sospesi, senza essere lavorati, finché un Utente non li approva o li rifiuta.

3.4 Il Titolare decide da solo quali dati affidare a Trailgun e ne garantisce la liceità, l'esattezza e la pertinenza rispetto alla pratica (art. 5 GDPR). Trailgun non verifica il contenuto dei documenti se non per svolgere le lavorazioni richieste.

Art. 4 Oggetto, natura, finalità e durata

4.1 Trailgun tratta i Dati delle Pratiche al solo fine di erogare il Servizio: ricezione e conservazione dei documenti, estrazione e riconoscimento del testo, trascrizione degli audio, classificazione, analisi, ricerca nei documenti, raccolta strutturata dei dati con le loro fonti, redazione degli Elaborati, controlli di qualità, comunicazioni attivate dal Titolare, assistenza, esportazione e cancellazione.

4.2 Interessati, categorie di dati, operazioni, luoghi e tempi di conservazione sono descritti nell'Allegato 1.

4.3 Il trattamento dura quanto il Contratto, più il tempo necessario alla restituzione e alla cancellazione dell'art. 17.

Art. 5 Istruzioni del Titolare

5.1 Trailgun tratta i Dati delle Pratiche soltanto su istruzione documentata del Titolare, anche per i trasferimenti verso paesi terzi, salvo che lo richieda il diritto dell'Unione o di uno Stato membro; in tal caso informa il Titolare prima del trattamento, se la legge non lo vieta per rilevanti motivi di interesse pubblico.

5.2 Sono istruzioni documentate: il Contratto e questo accordo; le impostazioni della Piattaforma e le azioni che il Titolare e i suoi Utenti vi compiono, come caricare un documento, avviare una lavorazione, attivare un'opzione, inviare una richiesta, cancellare una pratica; le richieste scritte del Titolare. Le istruzioni ulteriori che comportano costi o modifiche del Servizio si concordano per iscritto.

5.3 Trailgun informa immediatamente il Titolare se ritiene che un'istruzione violi il GDPR o altre norme sulla protezione dei dati, e non la esegue finché il Titolare non la conferma in forma conforme o la modifica.

5.4 Trailgun non tratta i Dati delle Pratiche per finalità proprie. Se lo facesse, ne sarebbe considerato titolare per quel trattamento, ai sensi dell'art. 28, par. 10, GDPR.

Art. 6 Obblighi del Titolare

6.1 Il Titolare garantisce di disporre di una base giuridica valida per il trattamento dei Dati delle Pratiche e per il loro affidamento a un responsabile, e di aver fornito agli interessati le informazioni dovute ai sensi degli artt. 13 e 14 GDPR, nei limiti dell'art. 14, par. 5, lett. b) e d), per i dati coperti dal segreto professionale.

6.2 Il Titolare carica soltanto documenti che ha il diritto di trattare e di affidare a Trailgun, nel rispetto del segreto professionale e del dovere di riservatezza (art. 28 del Codice deontologico forense), del segreto bancario e degli altri obblighi che lo vincolano. Il professionista informa i propri clienti dell'uso di sistemi di intelligenza artificiale nella misura richiesta dall'art. 13 della legge 132/2025.

6.3 Il Titolare tratta i dati relativi a condanne penali e reati (art. 10 GDPR) e le categorie particolari di dati (art. 9 GDPR) contenuti nei documenti solo in presenza di una condizione di liceità, in particolare per accertare, esercitare o difendere un diritto in sede giudiziaria (art. 9, par. 2, lett. f, GDPR e art. 2-octies, comma 3, lett. e, del Codice), e nel rispetto delle Regole deontologiche per lo svolgimento di investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria. Non carica categorie particolari di dati oltre quanto serve alla pratica.

6.4 Il Titolare è responsabile delle misure di sua competenza: l'abilitazione e la disattivazione degli Utenti, la custodia delle credenziali e delle chiavi di accesso, la configurazione della visibilità dei clienti dello studio, la sicurezza dei propri dispositivi e delle proprie caselle email.

6.5 Il Titolare impartisce istruzioni conformi alla normativa e rivede gli Elaborati prima di usarli (art. 11).

Art. 7 Divieto di addestramento e di riuso

7.1 Trailgun non usa i Dati delle Pratiche, i documenti né gli Elaborati per addestrare, ottimizzare o valutare modelli di intelligenza artificiale, propri o di terzi, né per finalità proprie diverse dal Servizio.

7.2 Tutti i modelli, compresi quelli per gli embeddings, sono eseguiti su Amazon Bedrock nella regione di Francoforte, nell'Unione europea, a condizioni che escludono la conservazione di input e output oltre il tempo dell'elaborazione (compresa la cache del prompt dell'analisi estesa, di un'ora, nella stessa regione), il loro uso per l'addestramento e l'accesso del produttore del modello. Una policy di AWS Organizations esclude inoltre i contenuti di Bedrock, Textract e Transcribe dal miglioramento dei servizi di AWS.

7.3 Gli Elaborati di un cliente non vengono usati per produrre Elaborati per altri clienti. Le regole che il Titolare chiede di ricordare per i propri atti futuri restano nella sua organizzazione. I miglioramenti generali della Piattaforma si basano su segnalazioni e correzioni prive di dati personali.

7.4 Trailgun non sposta l'esecuzione dei modelli fuori dall'Unione europea; un cambiamento del fornitore dei modelli segue l'art. 12.

Art. 8 Riservatezza e segreto professionale

8.1 Trailgun autorizza al trattamento soltanto le persone che ne hanno bisogno per il loro compito, le designa per iscritto ai sensi dell'art. 29 GDPR e dell'art. 2-quaterdecies del Codice, le istruisce e le vincola alla riservatezza con un obbligo contrattuale o di legge.

8.2 Trailgun riconosce che i Dati delle Pratiche possono essere coperti dal segreto professionale dell'avvocato o dal segreto bancario e li tutela con il medesimo rigore. Il personale di Trailgun accede al contenuto dei documenti solo quando serve per un'assistenza richiesta dal Titolare o per gestire un incidente. Ogni accesso amministrativo all'infrastruttura è registrato e conservato 12 mesi, e ogni accesso del personale al contenuto delle pratiche è annotato nel registro degli accessi del personale, di cui il Titolare può chiedere l'estratto che lo riguarda.

8.3 Trailgun revoca gli accessi di una persona entro 24 ore dalla cessazione del suo rapporto.

8.4 Gli obblighi di riservatezza sopravvivono alla cessazione dell'accordo senza limiti di tempo.

Art. 9 Sicurezza del trattamento

9.1 Trailgun adotta le misure tecniche e organizzative dell'Allegato 2, adeguate al rischio ai sensi dell'art. 32 GDPR, tenuto conto della natura dei dati, compresi quelli giudiziari, e le aggiorna nel tempo senza ridurne il livello complessivo.

9.2 Trailgun verifica periodicamente l'efficacia delle misure, con prove di ripristino trimestrali documentate da un verbale e test automatici a ogni rilascio, realizza le tappe del Percorso di certificazione e piattaforma (documento 12, versione 2.0) alle date ivi indicate, compreso il penetration test indipendente annuale (tappa R06), e informa il Titolare dei cambiamenti rilevanti.

Art. 10 Fascicoli penali e dati giudiziari

10.1 Quando il Titolare indica che una pratica è di materia penale, o la Piattaforma la riconosce come tale, si applicano misure ulteriori: i passaggi dei documenti non vengono trasformati in rappresentazioni vettoriali per la ricerca (embeddings); consultazioni (una all'ora per utente), domande, analisi, confronti fra depositi, timeline, grafi e schede dell'imputato vanno in un registro degli accessi che il Titolare consulta ed esporta.

10.2 Le registrazioni audio e le intercettazioni che il Titolare carica si trascrivono nell'Unione europea e restano nella pratica come gli altri documenti.

10.3 Le schede e le analisi riferite a una persona (per esempio la scheda di un imputato) restano nella pratica in cui il Titolare le genera e si cancellano con essa: Trailgun non costruisce profili delle persone al di fuori della singola pratica.

10.4 Il testo dei fascicoli penali è elaborato solo su Amazon Bedrock nell'Unione (art. 7.2) e va al riconoscimento del testo di riserva (Allegato 3) solo se il Titolare lo attiva.

Art. 11 Intelligenza artificiale e supervisione umana

11.1 Gli agenti di Trailgun preparano bozze, analisi e segnalazioni che rimandano ai documenti da cui provengono; i dati che i documenti non riportano sono dichiarati «N/D». Nessun Elaborato è una decisione: lo rivede e lo adotta un professionista del Titolare.

11.2 La Piattaforma non prende decisioni basate unicamente su un trattamento automatizzato che producano effetti giuridici sugli interessati o che incidano in modo analogo su di loro (art. 22 GDPR) e non svolge profilazione.

11.3 Trailgun fornisce al Titolare, come utilizzatore del sistema, le informazioni necessarie a usarlo in modo conforme al Regolamento (UE) 2024/1689, raccolte nella Scheda di trasparenza del sistema (documento 09, AI Act e uso dell'IA nella professione).

11.4 I DOCX e PDF prodotti dagli agenti portano una marcatura leggibile da macchina (art. 50, par. 2, Regolamento (UE) 2024/1689); chat ed email automatiche dichiarano l'uso dell'IA (art. 50, par. 1).

Art. 12 Sub-responsabili 1341

12.1 Il Titolare autorizza in via generale il ricorso ai sub-responsabili dell'Allegato 3. Trailgun tiene aggiornata e fornisce su richiesta l'identità dei fornitori a valle di ciascun sub-responsabile, come previsto dal Parere EDPB 22/2024; pubblica l'elenco aggiornato su https://trailgun.ai/subprocessors e valuta ogni sub-responsabile prima dell'ingaggio e ogni anno.

12.2 Trailgun comunica per email all'amministratore e al DPO del Titolare, almeno 30 giorni prima, l'aggiunta o la sostituzione di un sub-responsabile, indicandone identità, attività, luogo del trattamento e garanzie.

12.3 Entro quel termine il Titolare può opporsi per motivi ragionevoli legati alla protezione dei dati. Le parti cercano in buona fede una soluzione; se non la trovano entro 30 giorni, il Titolare può recedere dal Contratto senza penali, con il rimborso dei corrispettivi pagati e non goduti, che costituisce il suo unico rimedio.

12.4 Trailgun impone a ogni sub-responsabile, con contratto scritto, obblighi di protezione dei dati non meno rigorosi di quelli di questo accordo e risponde verso il Titolare del loro adempimento (art. 28, par. 4, GDPR). I contratti scritti con i sub-responsabili dell'Allegato 3 sono in essere e si mostrano in sede di verifica.

12.5 Per il Titolare soggetto a DORA, quando il Servizio sostiene funzioni essenziali o importanti: il preavviso è di 60 giorni; il cambiamento non si attua prima della scadenza del preavviso né finché l'opposizione del Titolare è pendente; se il Titolare non si oppone entro il preavviso, il cambiamento si può attuare (art. 5 del Regolamento delegato (UE) 2025/532). Trailgun applica ai sub-responsabili rilevanti gli obblighi dell'art. 4 del medesimo Regolamento.

12.6 Ogni Titolare può chiedere, nelle condizioni particolari del Modulo d'ordine, un'autorizzazione specifica preventiva per determinate categorie di sub-responsabili: per quelle categorie il silenzio del Titolare vale come diniego e prevale sull'art. 12.5.

12.7 Se un sub-responsabile deve essere sostituito con urgenza perché cessa la sua attività o presenta un rischio per la sicurezza dei dati, Trailgun può sostituirlo con uno che offra garanzie almeno equivalenti e lo comunica entro 72 ore; resta il diritto di opposizione e di recesso dell'art. 12.3. La sostituzione urgente non si applica alle categorie dell'art. 12.6.

Art. 13 Trasferimenti verso paesi terzi

13.1 I Dati delle Pratiche sono conservati nell'Unione europea e vi sono elaborati, salvo i casi dell'Allegato 4. Un trasferimento verso un paese terzo avviene solo in quei casi o su nuova autorizzazione secondo l'art. 12.

13.2 Ogni trasferimento si basa su una decisione di adeguatezza o sulle clausole contrattuali tipo della Decisione di esecuzione (UE) 2021/914 della Commissione, con le misure supplementari che risultano necessarie dalla valutazione d'impatto del trasferimento. Dove un fornitore è certificato nel Data Privacy Framework UE-USA, le clausole contrattuali tipo restano in vigore come garanzia sostitutiva.

13.3 Trailgun ha svolto le valutazioni d'impatto dei trasferimenti dell'Allegato 4, le mette a disposizione del Titolare, le aggiorna e lo informa senza ritardo se cambiano le condizioni su cui si basano.

Art. 14 Richieste delle autorità

14.1 Se un'autorità pubblica chiede l'accesso ai Dati delle Pratiche, Trailgun la invita a rivolgersi al Titolare, informa il Titolare senza ritardo se la legge lo consente, verifica la legittimità della richiesta, la contesta se infondata e comunica solo i dati strettamente necessari. Non dà seguito alle richieste di autorità di paesi terzi che non si fondano su un accordo internazionale (art. 48 GDPR).

14.2 Trailgun documenta le richieste ricevute e, se la legge lo consente, ne informa il Titolare almeno una volta all'anno.

Art. 15 Assistenza al Titolare

15.1 Tenuto conto della natura del trattamento, Trailgun assiste il Titolare con misure adeguate per rispondere alle richieste di esercizio dei diritti degli interessati (artt. 15-22 GDPR). La Piattaforma consente al Titolare di consultare, esportare, correggere e cancellare i documenti e gli Elaborati di ogni pratica.

15.2 Trailgun inoltra al Titolare entro 3 giorni lavorativi le richieste che riceve direttamente dagli interessati e non vi risponde senza sua istruzione.

15.3 Trailgun fornisce al Titolare, entro 10 giorni lavorativi dalla richiesta, le informazioni di cui dispone per la valutazione d'impatto sulla protezione dei dati (art. 35 GDPR) e per l'eventuale consultazione preventiva (art. 36): descrizione del trattamento, flussi, misure di sicurezza, sub-responsabili, valutazioni dei trasferimenti e Scheda di trasparenza del sistema, oltre al supporto alla DPIA già compilato del documento 06, Allegato 2, e al modello compilabile del documento 50.

Art. 16 Violazioni dei dati personali

16.1 Trailgun notifica al Titolare una violazione dei Dati delle Pratiche senza ingiustificato ritardo e comunque entro 24 ore da quando ne ha avuto conoscenza, per email al referente sicurezza e al DPO indicati nel Modulo d'ordine. Al Titolare soggetto a DORA invia inoltre la notifica iniziale dell'incidente TIC entro 2 ore, per email e per telefono al referente, gli aggiornamenti almeno ogni 24 ore, la relazione intermedia entro 48 ore dalla notifica iniziale e la relazione finale entro 20 giorni dalla chiusura, come previsto dall'Allegato DORA (documento 18), con i modelli di notifica del documento 51.

16.2 La notifica descrive, per quanto già noto: la natura della violazione, le categorie e il numero approssimativo di interessati e di registrazioni, le probabili conseguenze, le misure adottate o proposte, un referente. Le informazioni non disponibili subito si forniscono per fasi, senza ulteriore ritardo (art. 33, par. 3 e 4, GDPR).

16.3 Trailgun coopera con il Titolare nella valutazione della violazione, nelle notifiche al Garante per la protezione dei dati personali e agli interessati (artt. 33 e 34 GDPR) e nelle misure di contenimento, e documenta la violazione. La notifica non costituisce riconoscimento di responsabilità.

16.4 Trailgun tiene un registro delle violazioni e ne fornisce al Titolare, su richiesta, l'estratto che lo riguarda.

Art. 17 Restituzione e cancellazione

17.1 Durante il Contratto il Titolare può cancellare in ogni momento una pratica o un cliente: la cancellazione è definitiva e riguarda documenti, testi estratti, trascrizioni, indici di ricerca, Elaborati, versioni, comunicazioni, domande e attività della pratica, la cache del testo riconosciuto, le conversazioni con gli agenti e i riferimenti ai contenuti negli eventi di costo.

17.2 Alla cessazione il Titolare sceglie tra la restituzione dei dati seguita dalla cancellazione e la sola cancellazione (art. 28, par. 3, lett. g, GDPR), e conserva per 30 giorni l'accesso in sola lettura per esportare i propri dati. Su richiesta, Trailgun fornisce entro 10 giorni lavorativi un'esportazione complessiva in archivio cifrato: documenti originali, Elaborati in DOCX e PDF/A, testi estratti, dati strutturati in JSON e CSV, registri in CSV, indice con impronte SHA-256, con il certificato di restituzione (documento 53). Per il Titolare cui si applica l'Allegato DORA i termini decorrono dalla fine del periodo di transizione, fino a 12 mesi.

17.3 Nei 30 giorni successivi Trailgun cancella tutti i dati del Titolare dalla Piattaforma e dai sistemi dei sub-responsabili, compresi testi estratti, cache del testo riconosciuto, conversazioni con gli agenti, indici, registri delle lavorazioni e utenti, e ne dà conferma scritta entro 5 giorni lavorativi dalla cancellazione con il certificato di cancellazione (documento 54). Le copie di sicurezza, comprese quelle prima dei rilasci, escono dalla rotazione entro 14 giorni dalla cancellazione: in tutto, al massimo 74 giorni dalla cessazione.

17.4 Restano esclusi i soli dati che il diritto dell'Unione o nazionale obbliga a conservare, per il tempo previsto e senza ulteriore trattamento; i dati di fatturazione dello studio, che non sono Dati delle Pratiche, si conservano 10 anni (art. 2220 c.c.).

Art. 18 Informazioni e verifiche 1341

18.1 Trailgun mette a disposizione del Titolare le informazioni necessarie a dimostrare il rispetto dell'art. 28 GDPR e consente le verifiche, comprese le ispezioni, svolte dal Titolare o da un revisore da questi incaricato e vincolato alla riservatezza.

18.2 Le verifiche ordinarie si svolgono una volta all'anno, con 30 giorni di preavviso, in orario lavorativo, fino a 2 giorni in loco e senza compromettere la sicurezza e la riservatezza degli altri clienti. Si parte dalla documentazione e dai questionari, ai quali Trailgun risponde entro 15 giorni lavorativi, uno all'anno senza costi. Le verifiche straordinarie si svolgono dopo un incidente grave o su richiesta di un'autorità, con 5 giorni lavorativi di preavviso. Ciascuna parte sostiene i propri costi. La richiesta si può presentare con il modulo del documento 52.

18.3 Per il Titolare soggetto a DORA, quando il Servizio sostiene funzioni essenziali o importanti, e per le autorità competenti, i diritti di accesso, ispezione e audit sono illimitati, con il diritto di fare copie, anche in forma congiunta con altri clienti (art. 30, par. 3, lett. e, del Regolamento (UE) 2022/2554; art. 8 del d.lgs. 23/2025), come previsto dall'Allegato DORA (documento 18).

Art. 19 Registro e cooperazione con l'autorità

19.1 Trailgun tiene il registro delle categorie di attività di trattamento svolte per conto del Titolare (art. 30, par. 2, GDPR; documento 40), ne fornisce su richiesta l'estratto che lo riguarda e coopera, su richiesta, con il Garante per la protezione dei dati personali (art. 31).

Art. 20 Responsabilità 1341

20.1 Ciascuna parte risponde dei danni causati dal trattamento secondo l'art. 82 GDPR. Trailgun risponde soltanto se non ha adempiuto gli obblighi del GDPR specificamente diretti ai responsabili o ha agito in modo difforme o contrario alle istruzioni legittime del Titolare.

20.2 Nei rapporti tra le parti si applica il limite maggiorato dell'art. 17.3 delle Condizioni generali; il limite non si applica in caso di dolo o colpa grave (art. 1229 c.c.) né dove la legge non lo consente.

Art. 21 Durata, prevalenza e disposizioni finali 1341

21.1 L'accordo decorre dalla sottoscrizione, dura quanto il Contratto e, dopo, finché Trailgun tratta Dati delle Pratiche per conto del Titolare.

21.2 Per i dati personali l'accordo prevale sugli altri documenti contrattuali, salvo l'Allegato DORA (documento 18) per accesso, ispezione, notifica degli incidenti e strategia di uscita.

21.3 Le modifiche si fanno per iscritto. Trailgun può aggiornare gli Allegati 2 e 3 secondo gli artt. 9 e 12; le modifiche imposte dalla legge, da un'autorità o dall'adozione di nuove clausole contrattuali tipo si applicano dalla data prevista.

21.4 L'accordo è regolato dalla legge italiana. Per ogni controversia è competente in via esclusiva il Foro di [città della sede di Trailgun], salve le norme inderogabili.

21.5 Trailgun realizza le tappe del Percorso di certificazione e piattaforma (documento 12, versione 2.0) richiamate in questo accordo e nei suoi Allegati alle date ivi indicate. Comunica al Titolare il raggiungimento di ciascuna tappa e, se una data non può essere rispettata, il motivo e la nuova data prima della scadenza.

SOTTOSCRIZIONE

Letto, confermato e sottoscritto

Il Titolare designa Trailgun responsabile del trattamento dei Dati delle Pratiche alle condizioni di questo accordo e dei suoi allegati; Trailgun accetta. L'accordo può essere sottoscritto con firma digitale o con firma autografa, anche in due esemplari.

LUOGO

DATA

IL TITOLARE

[Studio legale, banca, intermediario o servicer]

Firma — nome e qualità del firmatario

IL RESPONSABILE

[Trailgun S.r.l.] , in persona di Franco Puppo, CEO e legale rappresentante

Firma — Franco Puppo

Approvazione specifica delle clausole

Ai sensi e per gli effetti degli artt. 1341 e 1342 del codice civile, il Titolare dichiara di aver letto con attenzione e di approvare specificamente le seguenti clausole dell'accordo:

Art. 12.3 opposizione a un nuovo sub-responsabile e recesso come unico rimedio;
Art. 12.5 attuazione del cambiamento di sub-responsabile in assenza di opposizione entro il preavviso;
Art. 12.6 silenzio come diniego per le categorie di fornitori soggette ad autorizzazione specifica;
Art. 12.7 sostituzione urgente di un sub-responsabile con comunicazione entro 72 ore;
Art. 18.2 frequenza, preavviso, modalità e costi delle verifiche;
Art. 20.2 limitazione della responsabilità nei rapporti tra le parti;
Art. 21.3 aggiornamento degli Allegati 2 e 3 da parte di Trailgun;
Art. 21.4 legge applicabile e foro competente esclusivo.

IL TITOLARE, PER APPROVAZIONE SPECIFICA

Firma

Allegati: 1. Descrizione del trattamento · 2. Misure tecniche e organizzative · 3. Sub-responsabili autorizzati · 4. Trasferimenti verso paesi terzi. Documenti collegati: Condizioni generali di servizio e Modulo d'ordine; 18 Allegato DORA; 06 Protezione dei dati personali; 40 Registro dei trattamenti del responsabile; 50 Supporto alla DPIA; 09 AI Act, con la Scheda di trasparenza del sistema; 12 Percorso di certificazione e piattaforma; 46 Mappa GDPR art. 28; 58 versione modificabile di questo accordo.

ALLEGATO 1

Descrizione del trattamento

Art. 28, par. 3, GDPR. Si completa con la sezione 9 del Modulo d'ordine, dove il Titolare indica interessati e categorie di dati delle proprie pratiche.

VOCE	DESCRIZIONE
Titolare	Lo studio, la banca, l'intermediario o il servicer indicato in testa all'accordo (o il suo titolare, nel caso dell'art. 2.4)
Responsabile	[Trailgun S.r.l.] («Trailgun»), legale rappresentante Franco Puppo, CEO; referente privacy privacy@trailgun.ai; DPO [...]
Finalità	Preparazione di atti, analisi e verifiche per l'attività del Titolare, nelle lavorazioni che attiva: decreti ingiuntivi, insinuazioni al passivo, escussione di garanzie pubbliche, remediation di data tape, assessment e due diligence su crediti, analisi del faldone con domande e funzioni sul fascicolo, trattative, revisione in Word, ricerca di fonti giuridiche
Origine dei dati	Esclusivamente il Titolare e i suoi Utenti, tramite i canali dell'art. 3.1; per conto e su istruzione del Titolare, le risposte dei suoi clienti, le visure richieste e i messaggi delle trattative (art. 3.2)
Operazioni	Raccolta tramite caricamento, archivi di pratiche, caselle email dedicate e API; conservazione; estrazione e riconoscimento del testo, con le coordinate sulla pagina; separazione dei PDF che contengono più atti; trascrizione degli audio con distinzione dei parlanti; classificazione; indicizzazione per la ricerca (senza embeddings sulle pratiche penali); analisi; raccolta strutturata dei dati con le fonti; redazione e controllo degli Elaborati; comunicazioni attivate dal Titolare; esportazione; cancellazione
Interessati	Clienti del Titolare e loro rappresentanti; debitori, debitori ceduti, garanti e fideiussori; controparti e loro difensori; parti di contratti e trattative; organi delle procedure; indagati, imputati, persone offese, testimoni e altri soggetti di procedimenti penali, comprese le persone intercettate; dipendenti e collaboratori del Titolare; altre persone citate nei documenti
Categorie di dati	Anagrafici e di contatto; codici fiscali e documenti d'identità; dati di rapporti contrattuali e bancari (contratti, fatture, estratti conto, piani di ammortamento, garanzie); dati economici, patrimoniali e fiscali; dati per debitore e per rapporto dei data tape; dati relativi a procedure giudiziarie, concorsuali e amministrative; registrazioni audio, voce e loro trascrizioni; contenuto di comunicazioni e conversazioni intercettate
Dati particolari e giudiziari	Dati relativi a condanne penali e reati (art. 10 GDPR) nella misura in cui risultano dagli atti, con le misure dell'art. 10 dell'accordo; categorie particolari (art. 9 GDPR) solo occasionalmente e nei limiti dell'art. 6.3. I dati su procedure civili e concorsuali sono dati comuni
Natura e frequenza	Trattamento continuativo, automatizzato tramite agenti di intelligenza artificiale, con revisione umana degli Elaborati da parte del Titolare; nessuna decisione automatizzata ai sensi dell'art. 22 GDPR, nessuna profilazione
Conservazione	Per la durata del Contratto o fino alla cancellazione della pratica da parte del Titolare; poi secondo l'art. 17, al massimo 74 giorni dalla cessazione. File temporanei per il riconoscimento del testo e la trascrizione: 1 giorno. Copie di sicurezza, comprese quelle prima dei rilasci: 14 giorni ciascuna
Luogo	Dati a riposo nell'Unione europea: Germania (AWS, Francoforte), copie di sicurezza in Irlanda (AWS, Dublino). Riconoscimento del testo e trascrizione a Francoforte. Modelli ed embeddings: Amazon Bedrock nella regione di Francoforte. Eccezioni nell'Allegato 4

ALLEGATO 2

Misure tecniche e organizzative

Art. 32 GDPR. Le misure sono in essere alla sottoscrizione; le tappe successive sono indicate con il codice del Percorso di certificazione e piattaforma (documento 12) e vincolano Trailgun secondo l'art. 21.5. Il dettaglio è nel documento 06, § 10, e nel documento 05.

AREA	MISURE	STATO
Infrastruttura	Amazon Web Services, regione eu-central-1 (Francoforte), in un account dedicato e intestato a Trailgun; ambienti di sviluppo e collaudo separati dalla produzione, con propri utenti, dati e servizi esterni simulati. Nessun accesso SSH, in ingresso solo le porte web (80, che reindirizza, e 443); amministrazione tramite AWS Systems Manager con sessioni registrate; infrastruttura come codice.	IN ESSERE più zone: R12
Cifratura	A riposo: volumi dei dati e di sistema e copie di sicurezza cifrati (AES-256, AWS KMS); archivio temporaneo per il riconoscimento del testo e la trascrizione cifrato, con accesso pubblico bloccato, solo TLS e scadenza a 1 giorno. In transito: HTTPS obbligatorio (TLS 1.2 o superiore) con certificati automatici, reindirizzamento da HTTP, HSTS di 1 anno e intestazioni di sicurezza.	IN ESSERE
Accesso degli Utenti	Solo su invito; autenticazione Amazon Cognito con protocollo SRP (la password non transita in chiaro e Trailgun non la conserva) e secondo fattore TOTP obbligatorio; ogni richiesta verificata sul token d'identità lato server; ruoli amministratore, membro, operator e viewer imposti dal server, permessi concessi dall'amministratore; visibilità di ogni cliente configurabile; disattivazione con blocco immediato dei nuovi accessi (una sessione aperta dura fino alla scadenza del token); chiavi API conservate come impronta e revocabili.	IN ESSERE
Separazione	Separazione logica per studio: ogni interrogazione sui dati di un cliente passa da un unico controllo di visibilità, con test dedicati. Cache del testo riconosciuto e del layout legate allo studio, mai condivise.	IN ESSERE
Fascicoli penali	Nessun embedding dei passaggi; registro degli accessi a consultazioni, domande, analisi, timeline, grafi e schede, consultabile dal Titolare (art. 10).	IN ESSERE
Modelli di IA	Modelli Claude ed embeddings Amazon Titan su Amazon Bedrock nelle regioni dell'Unione; regioni diverse rifiutate dal codice; nessun addestramento né da parte di Trailgun né del fornitore; opt-out di Bedrock, Textract e Transcribe dal miglioramento dei servizi di AWS; registri dei costi con solo modello, agente, quantità e costo, mai il testo; marcatura dei contenuti generati (art. 11.4).	IN ESSERE
Personale e accessi amministrativi	Accesso ai contenuti delle pratiche solo per assistenza richiesta o gestione di incidenti, registrato; privilegi minimi; credenziali amministrative temporanee con secondo fattore su tutte le console; registro degli accessi amministrativi 12 mesi; designazione e obbligo di riservatezza scritti; formazione all'ingresso e ogni anno; revoca entro 24 ore; revisione trimestrale degli accessi; operatori dell'assistenza limitati a ticket e base di conoscenza.	IN ESSERE responsabile della sicurezza dedicato: R13
Segreti	Credenziali dei servizi in AWS Systems Manager Parameter Store cifrato, mai nel codice; scansione dei segreti a ogni verifica; configurazione sul server leggibile solo dal servizio; rotazione ogni 12 mesi e all'uscita di una persona.	IN ESSERE
Notifiche	Le notifiche fuori dall'app (email, Telegram, SMS e WhatsApp) portano solo un avviso generico e il link, senza Dati delle Pratiche.	IN ESSERE
Integrità e qualità	Ogni dato dell'Elaborato rimanda al documento e alla pagina da cui proviene; i dati mancanti sono dichiarati «N/D»; ogni modifica conserva la versione precedente con autore e motivo; impronte SHA-256 dei file del pacchetto di deposito.	IN ESSERE
Registri	Log di accesso HTTP e applicativi 90 giorni, senza testo dei documenti, corpo delle richieste o token; 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'amministratore; registro degli accessi ai fascicoli penali.	IN ESSERE

AREA	MISURE	STATO
Rilevazione	Sonda esterna ogni minuto; allarmi 24/7 su salute, disco, CPU, memoria, errori e certificati; Amazon GuardDuty.	IN ESSERE
Ingresso dati	Limiti di dimensione e di numero dei file contro gli archivi malevoli; documenti da mittenti non riconosciuti trattenuti fino all'approvazione di un Utente; webhook verificati con firma in entrata e firmati in uscita; file aperti solo nel container dell'app, senza privilegi.	IN ESSERE
Continuità	Copia di sicurezza giornaliera alle 02:00 UTC, conservata 14 giorni e copiata cifrata in Irlanda; copie prima di ogni rilascio, conservate 14 giorni. RPO 24 ore, RTO 8 ore; prova di ripristino automatica a ogni verifica e trimestrale sullo snapshot reale, con verbale e RTO misurato; piano di continuità adottato e provato ogni anno.	IN ESSERE R01, R03, R11, R14
Cancellazione	Cancellazione completa di pratiche e clienti in ogni momento, compresi cache, conversazioni con gli agenti e riferimenti negli eventi di costo; strumento di cancellazione dello studio e degli utenti a fine contratto, con certificato.	IN ESSERE
Sviluppo e rilasci	Branch di ambiente protetti; controlli automatici obbligatori prima di ogni rilascio, anche manuale (tipi, test unitari e di interfaccia, scansione dei segreti, prova di ripristino); integrazione continua senza chiavi AWS; il rilascio si blocca se ci sono lavorazioni in corso; immagini analizzate per vulnerabilità; aggiornamenti delle dipendenze proposti ogni settimana e integrati con revisione. Correzioni: critiche 72 ore, alte 7 giorni, medie 30, basse 90.	IN ESSERE scansione esterna mensile: R05
Incidenti	Notifica al Titolare entro 24 ore; al Titolare soggetto a DORA notifica iniziale entro 2 ore, aggiornamenti ogni 24 ore, relazione intermedia in 48 ore e finale in 20 giorni; procedura con classificazione su tre livelli; registro degli incidenti e delle violazioni.	IN ESSERE
Verifiche e certificazioni	Infrastruttura certificata da AWS (ISO 27001, 27017, 27018, SOC 2, C5), rapporti su richiesta; verifiche del Titolare secondo l'art. 18.	IN ESSERE penetration test: R06; ISO/IEC 27001: R07, R08, R15, R16

ALLEGATO 3

Sub-responsabili autorizzati

Elenco al 01/12/2026, pubblicato e aggiornato su https://trailgun.ai/subprocessors e nel Registro dei subfornitori (documento 15). Le modifiche si comunicano 30 giorni prima, 60 per le funzioni DORA essenziali o importanti (art. 12).

FORNITORE	ATTIVITÀ	DATI	LUOGO E GARANZIE
Amazon Web Services EMEA SARL Lussemburgo	Infrastruttura e conservazione; autenticazione (Cognito) e invio dei codici d'accesso (SES); riconoscimento del testo (Textract); trascrizione degli audio (Transcribe); esecuzione dei modelli Claude di Anthropic e degli embeddings (Bedrock)	Tutti i documenti e gli Elaborati; dati degli Utenti	Germania (Francoforte); copie di sicurezza in Irlanda; modelli nella regione di Francoforte, dove il produttore del modello non accede ai dati. AWS GDPR DPA firmato; opt-out dei servizi di IA; nessun addestramento
Plus Five Five, Inc. (Resend) Stati Uniti	Email ai clienti del Titolare e nelle trattative, con le risposte; notifiche agli Utenti senza Dati delle Pratiche	Indirizzi, testi e allegati delle email	Invio e ricezione in Irlanda; società USA. DPA firmato; Data Privacy Framework verificato, clausole tipo come garanzia sostitutiva; conservazione [giorni]; nessun addestramento
Wolters Kluwer Italia S.r.l. (One LEGALE) Italia	Banca dati giuridica per ricerca fonti e verifica giurisprudenziale, con l'account di Trailgun	Stringhe di ricerca senza nomi, codici fiscali, importi o altri Dati delle Pratiche	Italia. DPA firmato; regola in codice, con test, che toglie i dati delle pratiche dalle ricerche
Openapi S.p.A., con **Namirial S.p.A.** Italia	Firma digitale qualificata degli atti e visure camerali, solo se il Titolare le richiede	Il PDF da firmare e i dati del firmatario; i dati dell'impresa da visurare	Italia. Namirial è prestatore qualificato (eIDAS). DPA firmato

FORNITORE	ATTIVITÀ	DATI	LUOGO E GARANZIE
Hoss Inc. (DocuPipe) Stati Uniti	Riconoscimento del testo di riserva, solo per i documenti che Textract non riesce a leggere e solo se il Titolare lo attiva (spento di default)	Il singolo file non leggibile	Stati Uniti. DPA firmato; clausole tipo (modulo 3); valutazione del trasferimento; conservazione [giorni] ; nessun addestramento

Fornitori che non ricevono Dati delle Pratiche. Telegram, Twilio Inc. (SMS e WhatsApp) e Resend per le notifiche consegnano agli Utenti che li scelgono solo un avviso generico e il link. Stripe tratta i soli dati di pagamento dello studio, come titolare autonomo. Google Workspace ospita le caselle delle persone di Trailgun, senza dati dalla Piattaforma. GitHub, Let's Encrypt, Docker Hub e npm servono a codice, certificati e componenti, senza dati dei clienti. Anthropic produce i modelli Claude ma non riceve dati: i modelli girano su Amazon Bedrock.

Strumenti del Titolare. Nella revisione in Word il file passa dal browser dell'Utente al OneDrive o SharePoint del Titolare, secondo il suo contratto con Microsoft: Trailgun non ne riceve le credenziali e Microsoft non è un suo sub-responsabile.

ALLEGATO 4

Trasferimenti verso paesi terzi

Archivi, copie, modelli ed embeddings sono nell'Unione europea. Possono uscire solo le email delle comunicazioni attivate dal Titolare e, se lo attiva, i file letti dal motore di riserva. Le valutazioni d'impatto dei trasferimenti (accesso delle autorità statunitensi, contenzioso sul Data Privacy Framework) sono svolte e si forniscono su richiesta a privacy@trailgun.ai.

FORNITORE	CHE COSA PUÒ USCIRE	BASE DEL TRASFERIMENTO	MISURE SUPPLEMENTARI
Resend	Email ai clienti del Titolare e alle controparti, e risposte; possibile accesso della società USA	Data Privacy Framework (certificazione verificata); clausole contrattuali tipo come garanzia sostitutiva	Invio in Irlanda; cifratura in transito; le email partono solo se il Titolare attiva le comunicazioni; funzione disattivabile
DocuPipe	Singoli file non leggibili da Textract	Clausole contrattuali tipo, modulo 3	Solo di riserva e solo se il Titolare lo attiva; cifratura in transito; nessun addestramento
AWS	Nessun trasferimento previsto; possibile accesso della capogruppo per assistenza	Data Privacy Framework; clausole tipo dell'AWS GDPR DPA	Cifratura a riposo; dati e modelli nell'Unione; chiavi gestite da Trailgun con la nuova piattaforma (R12)

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

Documento 07 del pacchetto di conformità; versione modificabile: documento 58. Collegato al documento 06, Protezione dei dati personali, e al documento 18, Allegato DORA al contratto. Subfornitori: https://trailgun.ai/subprocessors.