Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO 26

VERSIONE 2.0 · DICEMBRE 2026

Procedura per le violazioni dei dati personali

Per i dati delle pratiche il Titolare è lo studio, la banca o il servicer, e Trailgun è responsabile del trattamento: la notifica al Garante e agli interessati spetta al Titolare, e Trailgun gli dà tutto ciò che serve, presto e per iscritto. Per i propri trattamenti Trailgun è titolare e notifica direttamente.

AVVISO AL TITOLARE	CLIENTE DORA	INFORMAZIONI	TRAILGUN TITOLARE
24 ore	anche la notifica di 2 ore	anche per fasi successive	Garante entro 72 ore

PROCEDURA 26 · PROC-26

Violazioni dei dati personali

Ogni incidente si esamina anche come possibile violazione dei dati personali. Un sospetto fondato basta per avvisare il Titolare: la certezza non si aspetta.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
PROC-26	DPO [DPO esterno: nome o società], con il Responsabile della sicurezza	Organo amministrativo, [data della delibera]	2.0 · stato al 01/12/2026

REVISIONE	DESTINATARI
annuale e dopo ogni violazione	DPO e Responsabile della sicurezza di Trailgun; DPO e referenti sicurezza dei Titolari

DOCUMENTI COLLEGATI

documento 07, Accordo sul trattamento dei dati (DPA); documento 25, Risposta agli incidenti; documento 06, Protezione dei dati personali; documento 40, Registro dei trattamenti del responsabile; documento 51, Modelli di notifica degli incidenti; politica P16, Fascicoli penali

1 Scopo e ambito

1.1 La procedura vale per ogni violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a dati personali trattati da Trailgun (art. 4, punto 12, GDPR), anche presso un subfornitore.

1.2 Distingue due ruoli. Per i dati delle pratiche Trailgun è **responsabile del trattamento** e avvisa il Titolare (paragrafi 3-5). Per i dati degli account degli utenti, dei contatti, del sito e della fatturazione Trailgun è **titolare** e notifica direttamente (paragrafo 6).

2 Ruoli

- **DPO**: guida la valutazione, redige l'avviso al Titolare e la notifica al Garante quando Trailgun è titolare, tiene il registro delle violazioni.
- **Responsabile della sicurezza**: gestisce l'incidente con il documento 25, fornisce i fatti tecnici, contiene il danno.
- **Organo amministrativo**: è informato di ogni violazione che richiede un avviso o una notifica.

3 Passi, quando Trailgun è responsabile

1 **Riconoscere.** Per ogni incidente il Gestore dell'incidente e il DPO si chiedono: sono coinvolti dati personali? di chi, di quale Titolare, di quale categoria? in che modo (riservatezza, integrità, disponibilità)? L'ora in cui Trailgun sa, o ha un sospetto fondato, che ci sono dati personali coinvolti è l'ora della conoscenza.

2 **Contenere** con il documento 25 e preservare le evidenze.

3 **Avvisare il Titolare entro 24 ore** dalla conoscenza, senza ingiustificato ritardo, per email al referente sicurezza e al DPO indicati nel Modulo d'ordine, con i contenuti del paragrafo 7. Per il Titolare soggetto a DORA vale anche la notifica iniziale di 2 ore degli incidenti TIC: se l'incidente è lo stesso, la notifica di 2 ore lo dice già e l'avviso delle 24 ore la completa.

4 **Completare per fasi** le informazioni non disponibili subito, senza ulteriore ritardo (art. 33, par. 4, GDPR), indicando che cosa è ancora in accertamento e quando arriverà.

5 **Assistere il Titolare** nella valutazione del rischio, nella notifica al Garante entro 72 ore (art. 33, par. 1) e nella comunicazione agli interessati se il rischio è elevato (art. 34), con tutti i dati di cui Trailgun dispone. Trailgun non comunica con gli interessati né con il Garante per conto del Titolare senza sua istruzione scritta.

6 **Documentare** nel registro delle violazioni: fatti, effetti, misure, comunicazioni con l'ora. Al Titolare si consegna l'estratto su richiesta.

7 **Imparare**: il riesame dell'incidente (documento 25) comprende le misure che riducono il rischio di una violazione simile.

4 Elementi per la valutazione del rischio

Tipo di violazione; natura e sensibilità dei dati, con particolare peso per i dati relativi a reati e alle intercettazioni (art. 10 GDPR), le categorie particolari (art. 9) e i dati bancari e creditizi; volume di dati e di interessati; facilità di identificazione; gravità e durata delle conseguenze; caratteristiche degli interessati (per esempio indagati, vittime, debitori, minori); se i dati erano cifrati e se la chiave è rimasta sicura; numero di studi coinvolti; effetti sul segreto professionale. **Una violazione che tocca un fascicolo penale si presume ad alto rischio** finché non si dimostra il contrario.

5 Quando la violazione nasce presso un subfornitore

I contratti con i subfornitori che trattano dati dei Clienti li obbligano ad avvisare Trailgun senza ingiustificato ritardo (art. 28, par. 4, GDPR). L'ora in cui Trailgun riceve l'avviso è l'ora della conoscenza; Trailgun inoltra al Titolare quanto ricevuto e gestisce il subfornitore per ottenere le informazioni mancanti. Il registro dei subfornitori (documento 15) indica per ciascuno il contatto per gli incidenti.

6 Quando Trailgun è titolare

6.1 Per i dati degli account degli utenti, dei contatti, del sito e della fatturazione, Trailgun notifica la violazione al Garante entro 72 ore dalla conoscenza, salvo che sia improbabile che presenti un rischio per i diritti e le libertà delle persone, con la procedura telematica dell'autorità; se la notifica arriva oltre le 72 ore, indica i motivi del ritardo.

6.2 Se il rischio è elevato, comunica la violazione agli interessati senza ingiustificato ritardo, con linguaggio semplice: natura della violazione, contatto del DPO, probabili conseguenze, misure adottate e consigli (per esempio cambiare la password o riconfigurare l'app di autenticazione).

6.3 Ogni violazione, anche non notificata, si documenta nel registro con la motivazione della scelta (art. 33, par. 5).

7 · AVVISO AL TITOLARE · ENTRO 24 ORE	CHE COSA SCRIVERE	CONTENUTO
Codice e collegamento	VDP-aaaa-nnn; codice dell'incidente INC collegato	
Data e ora della violazione e della conoscenza	anche stimate; motivo di eventuali ritardi	
Natura della violazione	riservatezza, integrità, disponibilità; come è avvenuta	
Categorie e numero approssimativo di interessati	clienti dello studio, debitori, garanti, indagati, terzi	
Categorie e numero approssimativo di registrazioni	documenti, pratiche, campi; dati degli artt. 9 e 10	
Probabili conseguenze	per le persone e per il segreto professionale	
Misure adottate o proposte	contenimento, attenuazione degli effetti, prevenzione	
Subfornitori coinvolti	se la violazione è avvenuta presso un fornitore	
Informazioni in accertamento	e quando arriveranno	
Contatto	DPO di Trailgun e Responsabile della sicurezza	

8 Registro delle violazioni

Tenuto dal DPO di Trailgun, per tutte le violazioni, notificate o no: codice, Titolare, fatti, categorie e numero di interessati e registrazioni, conseguenze, misure, ora della conoscenza e di ogni comunicazione, valutazione del rischio e sua motivazione, esito. Al Titolare si consegna l'estratto delle voci che lo riguardano, su richiesta e in audit.

9 Altri impegni verso il Titolare

Le richieste degli interessati che arrivano a Trailgun si inoltrano al Titolare entro 3 giorni lavorativi, senza rispondere senza sua istruzione (documento 27). Le informazioni per la valutazione d'impatto del Titolare si forniscono entro 10 giorni lavorativi dalla richiesta (documento 50).

10 Riferimenti

GDPR, art. 4, punto 12, art. 28, par. 3, lett. f), e par. 4, artt. 33 e 34; Linee guida EDPB 9/2022 sulla notifica delle violazioni dei dati personali; DORA, art. 19 e art. 30, par. 2, lett. f), per il coordinamento con la notifica degli incidenti TIC; ISO/IEC 27001:2022, controllo 5.34 (privacy e protezione dei dati personali).

Trailgun

On target.

In a flash.

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

SICUREZZA E INCIDENTI, 24/7
security@trailgun.ai

REPERIBILITÀ PRIORITÀ 1
[+39 ...]

PRIVACY E DPO
privacy@trailgun.ai

Procedura 26 del pacchetto di conformità Trailgun, versione 2.0, stato al 01/12/2026. Attua l'articolo del DPA sulle violazioni (documento 07) e si coordina con la procedura di risposta agli incidenti (documento 25). Documento riservato, destinato al Cliente, al suo DPO e alle sue autorità di vigilanza.