SECURITY & COMPLIANCE

Sintesi della valutazione d’impatto sulla protezione dei dati

Valutazione strutturata di necessità, proporzionalità, rischi e mitigazioni.

Prodotto	ClaimEvidence
Codice	CLE-PUB-16-IT
Edizione documentale	Edizione del 30 agosto 2026
Efficacia / riesame	2026-08-30 / 2027-02-28
Titolare del documento	Nil Tech Europe S.r.l. · Compliance & Security
Classificazione	Pubblico

Preambolo, natura ed efficacia del documento

Nil Tech Europe S.r.l., con sede legale in Via Calmaggiore 5, 31100 Treviso (TV), Italia, P. IVA IT 05614380268 (di seguito «Niltech»), adotta il presente documento al fine di sintetizzare descrizione, necessità, proporzionalità, rischi per le persone, misure, rischio residuo e decisione della DPIA controllata.

Il documento è un atto societario di trasparenza e accountability. Non costituisce certificazione di terza parte, parere legale destinato a soggetti diversi dalla società, garanzia assoluta di sicurezza o dichiarazione generalizzata di conformità; gli impegni contrattuali derivano esclusivamente dagli accordi applicabili.

La sintesi riflette il metodo previsto dall’articolo 35 GDPR e dalle Linee guida WP248 rev.01. La valutazione completa resta un atto di accountability controllato; ove permanga un rischio elevato non mitigabile, il trattamento non può essere avviato senza le determinazioni richieste dall’articolo 36 GDPR.

Ambito soggettivo e oggettivo

Il perimetro oggettivo comprende ClaimEvidence, le relative interfacce pubbliche e i trattamenti strettamente connessi alle funzionalità descritte. Il sito istituzionale e la libreria documentale sono pubblicati su claimevidence.tech; il servizio applicativo è accessibile sul distinto dominio app.claimevidence.tech. Hostinger fornisce l’infrastruttura e, secondo la configurazione applicabile, il trasporto della posta. MySQL/MariaDB è software eseguito nell’ambiente controllato e non un sub-responsabile autonomo salvo distinto servizio gestito. OpenAI presta il servizio API soltanto per le funzioni abilitate; un eventuale fornitore email separato deve essere identificato e qualificato prima dell’uso.

Le operazioni considerate riguardano raccolta guidata di fotografie e documenti, organizzazione per pratica, controlli di completezza, supporto analitico configurabile, revisione umana ed esportazione. Le categorie di informazioni potenzialmente interessate sono: richieste demo e security pack sul sito; nell’applicazione, identificativi pratica, contatti autorizzati, fotografie, documenti, note, metadati di sessione e output assistiti. L’effettivo ruolo privacy, il titolo giuridico e l’ampiezza del trattamento dipendono dal rapporto contrattuale e dalle istruzioni lecite del soggetto che determina finalità e mezzi essenziali.

Definizioni e criteri interpretativi

- «Servizio»: l’insieme delle funzionalità di ClaimEvidence rese disponibili in base al contratto.
- «Cliente»: la persona giuridica o il professionista che conclude il contratto con Niltech.
- «Utente autorizzato»: la persona fisica abilitata dal Cliente a utilizzare il Servizio sotto la sua responsabilità.
- «Dati del Cliente»: dati, documenti, immagini, istruzioni e ogni altro contenuto conferito o generato per conto del Cliente.

- «Output assistito»: risultato elaborato mediante regole automatizzate o componenti di intelligenza artificiale, soggetto ai controlli indicati.
- «Fornitore ulteriore»: soggetto terzo che presta a Niltech un servizio tecnico rilevante per il perimetro documentato.
- «Incidente»: evento che compromette o può compromettere riservatezza, integrità, disponibilità, autenticità o resilienza.
- «Giorno lavorativo»: ogni giorno diverso da sabato, domenica o festività nazionale italiana.

Obblighi e presidi specifici

1. Niltech, nei limiti del ruolo assunto e ferme le responsabilità del Cliente, provvede a mappare finalità, ruoli, interessati, dati, fonti, destinatari e flussi. Owner, perimetro, dipendenze, criterio di accettazione ed evidenza sono identificati nel fascicolo applicabile; in loro assenza il presidio non è considerato dimostrato.

2. Niltech, nei limiti del ruolo assunto e ferme le responsabilità del Cliente, provvede a documentare basi, trasparenza, minimizzazione, qualità e diritti. Owner, perimetro, dipendenze, criterio di accettazione ed evidenza sono identificati nel fascicolo applicabile; in loro assenza il presidio non è considerato dimostrato.

3. Niltech, nei limiti del ruolo assunto e ferme le responsabilità del Cliente, provvede a considerare dati particolari, vulnerabilità, scala, monitoraggio e nuove tecnologie. Owner, perimetro, dipendenze, criterio di accettazione ed evidenza sono identificati nel fascicolo applicabile; in loro assenza il presidio non è considerato dimostrato.

4. Niltech, nei limiti del ruolo assunto e ferme le responsabilità del Cliente, provvede a valutare rischi di accesso, esclusione, errore, bias e perdita di controllo. Owner, perimetro, dipendenze, criterio di accettazione ed evidenza sono identificati nel fascicolo applicabile; in loro assenza il presidio non è considerato dimostrato.

5. Niltech, nei limiti del ruolo assunto e ferme le responsabilità del Cliente, provvede a collegare misure a evidenze e valutarne l'efficacia. Owner, perimetro, dipendenze, criterio di accettazione ed evidenza sono identificati nel fascicolo applicabile; in loro assenza il presidio non è considerato dimostrato.

6. Niltech, nei limiti del ruolo assunto e ferme le responsabilità del Cliente, provvede a bloccare o consultare quando resta un rischio elevato non mitigabile. Owner, perimetro, dipendenze, criterio di accettazione ed evidenza sono identificati nel fascicolo applicabile; in loro assenza il presidio non è considerato dimostrato.

Perimetro e ruoli

Il sito istituzionale e la libreria documentale sono pubblicati su claimevidence.tech; il servizio applicativo è accessibile sul distinto dominio app.claimevidence.tech. Hostinger fornisce l’infrastruttura e, secondo la configurazione applicabile, il trasporto della posta. MySQL/MariaDB è software eseguito nell’ambiente controllato e non un sub-responsabile autonomo salvo distinto servizio gestito. OpenAI presta il servizio API soltanto per le funzioni abilitate; un eventuale fornitore email separato deve essere identificato e qualificato prima dell’uso.

Il cliente è normalmente titolare per i dati operativi; Niltech responsabile. Niltech è titolare per i propri dati amministrativi e di sicurezza.

Dati, finalità e basi

richieste demo e security pack sul sito; nell’applicazione, identificativi pratica, contatti autorizzati, fotografie, documenti, note, metadati di sessione e output assistiti

Finalità: raccolta guidata di fotografie e documenti, organizzazione per pratica, controlli di completezza, supporto analitico configurabile, revisione umana ed esportazione.

Basi e necessità devono essere confermate dal titolare per lo specifico uso; dati particolari richiedono condizione aggiuntiva.

Rischi e misure

Rischi: accesso improprio, divulgazione, retention eccessiva, output errato, perdita di controllo, trasferimento e dipendenza fornitore. Misure: minimizzazione, accesso, logging, contratti, revisione umana, gestione incidenti, retention e verifica fornitori.

Esito e consultazione

La DPIA completa è nel pack controllato. Il rischio residuo deve essere accettato dall'owner competente; se resta elevato senza mitigazioni adeguate, l'uso non procede e si valuta la consultazione dell'autorità.

Natura della sintesi e titolarità della decisione

La presente sintesi descrive il metodo e le aree che richiedono valutazione; non prova che una DPIA completa sia stata conclusa per ogni Cliente o configurazione. Il titolare è responsabile di stabilire se il trattamento possa presentare un rischio elevato e, in tal caso, di completare la valutazione prima del trattamento. Niltech fornisce le informazioni ragionevolmente disponibili quale responsabile.

La DPIA deve descrivere operazioni, finalità e legittimo interesse; valutare necessità e proporzionalità; considerare rischi per diritti e libertà e relative fonti; definire misure, garanzie e meccanismi dimostrativi; raccogliere, ove opportuno, il punto di vista degli interessati; riportare parere del DPO se designato e decisione del titolare.

Fattori di rischio da esaminare

Fotografie, documenti e metadati di una pratica possono rivelare volti, targhe, ubicazioni, condizioni di salute, informazioni su minori o soggetti estranei alla pratica. Il Cliente deve definire istruzioni di raccolta che evitino riprese eccedenti, oscurare gli elementi non necessari quando ragionevole e documentare le condizioni applicabili agli articoli 9 e 10 GDPR.

Sono inoltre considerati volume e durata, monitoraggio, vulnerabilità degli interessati, combinazione di fonti, trasferimenti, accesso di fornitori, possibilità di contestazione, errore dell'IA, dipendenza professionale, sicurezza, cancellazione e conseguenze materiali. Necessità e proporzionalità sono valutate rispetto ad alternative meno invasive.

Se, dopo le misure, permane un rischio elevato che il titolare non può ridurre, il trattamento non è avviato prima della consultazione dell'autorità ai sensi dell'articolo 36 GDPR. Il riesame è obbligatorio quando cambia il rischio, la finalità, il modello, il fornitore, il flusso o la normativa.

Ripartizione delle responsabilità e limiti di affidamento

Il Cliente garantisce, per quanto di propria competenza, la liceità dei dati e delle istruzioni conferite, l'abilitazione degli utenti, l'adeguatezza delle basi giuridiche e delle informative, nonché la verifica professionale degli output. Niltech resta responsabile delle attività direttamente poste sotto il proprio controllo e non assume le funzioni regolamentari, deontologiche o decisionali proprie del Cliente.

Gli output di ClaimEvidence hanno natura ausiliaria. Salvo patto espresso e le norme inderogabili, essi non costituiscono parere legale, perizia, decisione assicurativa, determinazione di responsabilità, valutazione creditizia o altro atto riservato. Il destinatario deve esaminare fonti, completezza, coerenza e conseguenze prima di utilizzarli.

Nessuna clausola limita responsabilità che non possa essere esclusa per legge. Fuori da tali ipotesi, imputazione, rimedi, limiti e criteri di quantificazione seguono il contratto applicabile, tenuto conto del concorso del danneggiato, dell'obbligo di mitigazione e della prevedibilità del danno secondo la legge regolatrice.

Prova, riesame, richieste e legge applicabile

Ogni affermazione materiale deve poter essere ricondotta a un contratto, una configurazione approvata, un registro, un verbale, un test, un log o altra evidenza attendibile. Dichiarazioni del fornitore e controlli propri di Niltech sono mantenuti distinti. L'assenza di incidenti non prova, da sola, l'efficacia di una misura.

Le revisioni sono datate, motivate e approvate. Una revisione successiva non modifica retroattivamente i fatti o gli impegni applicabili a periodi precedenti. Le copie pubblicate sono identificate mediante codice, data e impronta crittografica; tali elementi provano l'integrità della copia, non l'efficacia sostanziale dei controlli descritti.

Segnalazioni, richieste di chiarimento, esercizio di diritti e contestazioni possono essere inviati a info@nil-tech.net. Niltech verifica l'identità e la legittimazione quando necessario, registra la richiesta, risponde nei termini applicabili e comunica eventuali proroghe o dinieghi motivati.

Salvo diversa disposizione inderogabile o pattuizione scritta, la legge italiana disciplina l'interpretazione del documento. La versione italiana costituisce il testo di riferimento; la traduzione inglese è fornita per agevolare la consultazione.

Fonti ufficiali e data normativa

Riferimenti verificati al 2026-08-30. L'applicabilità, il ruolo e le eventuali decorrenze devono essere nuovamente accertati sul caso concreto.

- Regolamento (UE) 2016/679 (GDPR)
- Linee guida WP248 rev.01 sulla valutazione d'impatto
- Garante per la protezione dei dati personali — Valutazione d'impatto sulla protezione dei dati