SECURITY & COMPLIANCE

Matrice di applicabilità e presidi di adeguamento normativo

Matrice datata di applicabilità, responsabilità ed evidenze richieste.

Prodotto	ClaimEvidence
Codice	CLE-PUB-24-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 mantenere una valutazione motivata di applicabilità, ruolo, requisiti, evidenze, gap e azioni per i principali quadri normativi.

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 matrice è uno strumento di individuazione e governo dei requisiti, non un parere pro veritate né un’attestazione generale di conformità. Applicabilità, ruolo, obblighi e decorrenze sono verificati sulla base del fatto concreto e delle fonti ufficiali vigenti.

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 analizzare entità, settore, dimensione, territorio, ruolo e caso d'uso. 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 separare obblighi diretti, contrattuali, di filiera e buone pratiche. 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 collegare ogni requisito a owner, controllo ed evidenza. 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 registrare gap, rischio, priorità, scadenza e dipendenze. 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 verificare fonti ufficiali e date di applicazione. 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 riesaminare dopo modifiche normative, contrattuali o tecniche. Owner, perimetro, dipendenze, criterio di accettazione ed evidenza sono identificati nel fascicolo applicabile; in loro assenza il presidio non è considerato dimostrato.

Metodo

L’applicabilità concreta dipende dal ruolo di Niltech, dal cliente, dal settore, dall’uso previsto, dalle categorie di dati e dalla configurazione. Le conclusioni sono riesaminate quando cambia uno di questi elementi.

La matrice è readiness, non parere legale o dichiarazione generale di conformità.

Matrice

Quadro	Valutazione	Evidenze / azioni
GDPR	Applicabile ai trattamenti di dati personali; ruoli variabili.	DPA, ROPA, DPIA, diritti, sicurezza, fornitori.
AI Act	Applicabilità e classe dipendono dall’uso previsto e dal ruolo nella catena.	Inventario, valutazione, trasparenza, supervisione, alfabetizzazione.
DORA	Direttamente per clienti finanziari; requisiti contrattuali e di due diligence possono ricadere sul fornitore ICT.	Scheda fornitore, incidenti, continuità, audit, uscita.
Data Act	Da valutare per portabilità, switching e clausole sui dati.	Export, uscita, catalogo dati, contratto.
NIS2	Da valutare per settore, dimensione, ruolo e catena di fornitura.	Risk management, incidenti, continuità, fornitori.
CRA	Da valutare rispetto alla qualificazione come prodotto con elementi digitali e al ruolo.	Secure development, vulnerabilità, aggiornamenti, reporting.

Perimetro giuridico e funzionale

I servizi di pagamento non rientrano nel perimetro descritto dalla presente documentazione.

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.

Riesame

Riesame semestrale e a ogni cambio rilevante di legge, ruolo, uso, dati, provider, architettura o incidente. Le azioni e le evidenze sono nel registro controllato.

Metodo di applicabilità

Per ciascuna fonte la matrice identifica soggetto obbligato, oggetto, territorio, ruolo, soglia o classificazione, obbligo, data di applicazione, evidenza, owner e conclusione motivata. Le categorie "applicabile", "non applicabile", "indirettamente rilevante" e "da determinare" non sono intercambiabili e la conclusione è riaperta al mutare dei fatti.

L'adozione volontaria di un presidio tratto da una norma non prova che la norma sia applicabile né che tutti i suoi requisiti siano soddisfatti. Analogamente, l'assenza da un perimetro diretto non elimina obblighi contrattuali o di filiera.

Quadro temporale verificato

- GDPR: applicabile dal 25 maggio 2018; ruoli e obblighi dipendono dal trattamento concreto
- DORA: applicabile dal 17 gennaio 2025 alle entità e relazioni ICT nel suo perimetro
- Data Act: applicabile dal 12 settembre 2025, ferme decorrenze ed eccezioni specifiche
- NIS2 in Italia: recepita dal D.lgs. 4 settembre 2024, n. 138; applicabilità subordinata a soggetto, settore e servizio
- AI Act: obblighi e divieti hanno decorrenze differenziate; trasparenza dell'articolo 50 applicabile dal 2 agosto 2026; sistemi ad alto rischio dell'allegato III dal 2 dicembre 2027 e dell'allegato I dal 2 agosto 2028, come modificato dal Regolamento (UE) 2026/1744
- Cyber Resilience Act: disposizioni sugli organismi di valutazione della conformità applicabili dall'11 giugno 2026, obblighi di reporting dall'11 settembre 2026 e principali obblighi dall'11 dicembre 2027, previa verifica del perimetro

Esito per il caso d'uso IA

La raccolta e organizzazione di evidenze di sinistro e il supporto alla revisione non determinano, in quanto tali, copertura, responsabilità o liquidazione e non sono qualificati in via astratta come impiego ad alto rischio. La classificazione deve essere riaperta se il sistema viene destinato a decidere o raccomandare autonomamente esiti che producono effetti giuridici o analogamente significativi.

L'esito non esonera dagli obblighi comunque applicabili, inclusi trasparenza, alfabetizzazione, protezione dati, sicurezza, tutela dei consumatori e correttezza professionale. Ogni nuova destinazione è sottoposta a change assessment prima dell'uso.

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)
- Regolamento (UE) 2024/1689 (AI Act)
- Regolamento (UE) 2026/1744 — Omnibus digitale sull’IA
- Commissione europea — Linee guida finali sugli obblighi di trasparenza dell’articolo 50 AI Act, luglio 2026
- Regolamento (UE) 2022/2554 (DORA)
- Regolamento (UE) 2023/2854 (Data Act)
- Direttiva (UE) 2022/2555 (NIS2)
- D.lgs. 4 settembre 2024, n. 138 — recepimento NIS2 in Italia
- Regolamento (UE) 2024/2847 (Cyber Resilience Act)
- Commissione europea — Quadro di attuazione e scadenze del Cyber Resilience Act, 27 luglio 2026

Controllo del documento: la copia identificata nel manifest mediante impronta SHA-256 costituisce l’edizione documentale pubblicata alla data indicata. Il sigillo in intestazione è un elemento grafico societario neutro e non costituisce firma digitale, attestazione di terza parte o certificazione.