



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 27 luglio 2026
Efficacia / riesame	2026-07-27 / 2027-01-27
Titolare del documento	Niltech Europe S.r.l. · Compliance & Security
Classificazione	Pubblico

Preambolo, natura ed efficacia del documento

Niltech Europe S.r.l., con sede legale in Via Calmaggione 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. L'infrastruttura Hostinger, il database relazionale, il trasporto di posta e le API OpenAI operano secondo le rispettive funzioni e condizioni contrattuali.

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 senza pregiudizio per le responsabilità del Cliente, provvede a analizzare entità, settore, dimensione, territorio, ruolo e caso d'uso. Il relativo adempimento è attuato secondo criteri di necessità, proporzionalità e tracciabilità, è assegnato a un soggetto responsabile ed è sostenuto da evidenze adeguate alla natura del rischio. Qualora l'adempimento dipenda da informazioni, autorizzazioni o attività del Cliente o di un fornitore, tale dipendenza è comunicata e registrata; l'assenza del presupposto impedisce di considerare il controllo pienamente operante.
2. Niltech, nei limiti del ruolo assunto e senza pregiudizio per le responsabilità del Cliente, provvede a separare obblighi diretti, contrattuali, di filiera e buone pratiche. Il relativo adempimento è attuato secondo criteri di necessità, proporzionalità e tracciabilità, è assegnato a un soggetto responsabile ed è sostenuto da evidenze adeguate alla natura del rischio. Qualora l'adempimento dipenda da informazioni, autorizzazioni o attività del Cliente o di un fornitore, tale dipendenza è comunicata e registrata; l'assenza del presupposto impedisce di considerare il controllo pienamente operante.
3. Niltech, nei limiti del ruolo assunto e senza pregiudizio per le responsabilità del Cliente, provvede a collegare ogni requisito a owner, controllo ed evidenza. Il relativo adempimento è attuato secondo criteri di necessità, proporzionalità e tracciabilità, è assegnato a un soggetto responsabile ed è sostenuto da evidenze adeguate alla natura del rischio. Qualora l'adempimento dipenda da informazioni, autorizzazioni o attività del Cliente o di un fornitore, tale dipendenza è comunicata e registrata; l'assenza del presupposto impedisce di considerare il controllo pienamente operante.
4. Niltech, nei limiti del ruolo assunto e senza pregiudizio per le responsabilità del Cliente, provvede a registrare gap, rischio, priorità, scadenza e dipendenze. Il relativo adempimento è attuato secondo criteri di necessità, proporzionalità e tracciabilità, è assegnato a un soggetto responsabile ed è sostenuto da evidenze adeguate alla natura del rischio. Qualora l'adempimento dipenda da informazioni, autorizzazioni o attività del Cliente o di un fornitore, tale dipendenza è comunicata e registrata; l'assenza del presupposto impedisce di considerare il controllo pienamente operante.
5. Niltech, nei limiti del ruolo assunto e senza pregiudizio per le responsabilità del Cliente, provvede a verificare fonti ufficiali e date di applicazione. Il relativo adempimento è attuato secondo criteri di necessità, proporzionalità e tracciabilità, è assegnato a un soggetto responsabile ed è sostenuto da evidenze adeguate alla natura del rischio. Qualora l'adempimento dipenda da informazioni, autorizzazioni o attività del Cliente o di un fornitore, tale dipendenza è comunicata e registrata; l'assenza del presupposto impedisce di considerare il controllo pienamente operante.
6. Niltech, nei limiti del ruolo assunto e senza pregiudizio per le responsabilità del Cliente, provvede a riesaminare dopo modifiche normative, contrattuali o tecniche. Il relativo adempimento è attuato secondo criteri di necessità, proporzionalità e tracciabilità, è assegnato a un soggetto responsabile ed è sostenuto da evidenze adeguate alla natura del rischio. Qualora l'adempimento dipenda da informazioni, autorizzazioni o attività del Cliente o di un fornitore, tale dipendenza è comunicata e registrata; l'assenza del presupposto impedisce di considerare il controllo pienamente operante.

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. L'infrastruttura Hostinger, il database relazionale, il trasporto di posta e le API OpenAI operano secondo le rispettive funzioni e condizioni contrattuali.

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.

Ambito, destinatari e valore del documento

Questo documento è destinato a clienti, prospect, utenti autorizzati, consulenti e funzioni di controllo che devono comprendere il perimetro di ClaimEvidence. Il suo obiettivo specifico è mantenere una valutazione motivata di applicabilità, ruolo, requisiti, evidenze, gap e azioni per i principali quadri normativi. La descrizione si applica alla revisione documentale e alla data indicate e deve essere letta insieme a contratto, ordine, DPA, specifiche tecniche e procedure controllate applicabili.

Il sito istituzionale e la libreria documentale sono pubblicati su claimevidence.tech. Il servizio applicativo è accessibile sul distinto dominio app.claimevidence.tech. L'infrastruttura Hostinger, il database relazionale, il trasporto di posta e le API OpenAI operano secondo le rispettive funzioni e condizioni contrattuali.

In caso di divergenza prevalgono gli accordi sottoscritti e le configurazioni effettivamente approvate. Le informazioni pubbliche descrivono il programma di controllo e non trasformano capacità opzionali dei provider in controlli Niltech, né attestano automaticamente l'applicabilità o il soddisfacimento di una norma.

Definizioni operative

Le definizioni seguenti servono a interpretare il documento in modo coerente. I termini definiti dalla legge o dal contratto mantengono il significato attribuito dalla relativa fonte.

- Perimetro: sistemi, organizzazioni, dati e attività espressamente compresi nel documento.
- Owner: funzione responsabile di mantenere contenuto, evidenze, decisioni e riesami.
- Evidenza: registrazione verificabile, datata e riconducibile a un controllo o a una decisione.
- Eccezione: scostamento autorizzato, limitato nel tempo e accompagnato da misure compensative.
- Readiness: grado di preparazione documentato; non equivale a conformità certificata.

Requisiti e processo operativo

Il processo deve rimanere proporzionato al caso d'uso, ai dati, alle persone esposte e al possibile impatto. Per ClaimEvidence, le funzioni rilevanti comprendono raccolta guidata di fotografie e documenti, organizzazione per pratica, controlli di completezza, supporto analitico configurabile, revisione umana ed esportazione. Ogni fase deve avere un responsabile, input verificabili, criteri di completamento, evidenze e un percorso di escalation.

Prima dell'attivazione o della pubblicazione, l'owner verifica che i requisiti siano tradotti in controlli concreti e che i controlli siano effettivamente applicabili all'ambiente. Un controllo solo pianificato, una capacità non configurata o una dichiarazione generale del fornitore sono registrati come gap e non come misura operativa.

- analizzare entità, settore, dimensione, territorio, ruolo e caso d'uso
- separare obblighi diretti, contrattuali, di filiera e buone pratiche
- collegare ogni requisito a owner, controllo ed evidenza
- registrare gap, rischio, priorità, scadenza e dipendenze
- verificare fonti ufficiali e date di applicazione
- riesaminare dopo modifiche normative, contrattuali o tecniche

Ruoli e responsabilità

Niltech mantiene il documento, le configurazioni sotto il proprio controllo e il collegamento alle evidenze. Il cliente determina finalità, utenti, dati, autorizzazioni e decisioni professionali nel proprio perimetro. I provider rispondono delle componenti definite dai rispettivi contratti. I destinatari principali del prodotto sono studi, periti e organizzazioni che raccolgono e revisionano evidenze relative a sinistri.

Nessun ruolo è attribuito implicitamente. Owner di prodotto, sicurezza, privacy, continuità e IA devono essere identificati nel registro controllato. Quando una persona ricopre più ruoli, l'approvazione di rischi, eccezioni o risultati materiali deve



includere una verifica indipendente proporzionata.

- Direzione: approva rischio residuo, eccezioni materiali e priorità.
- Owner: mantiene requisiti, controlli, evidenze, gap e riesami.
- Operatori: seguono istruzioni, verificano input/output e segnalano anomalie.
- Cliente: assicura liceità, autorizzazioni, qualità dei dati e uso professionale.
- Fornitori: erogano i servizi e le informazioni previste dai relativi accordi.

Evidenze, verifiche e accountability

Ogni affermazione materiale deve essere riconducibile a un'evidenza corrente: configurazione, contratto, report, test, ticket, verbale, log o registro. Le evidenze sono classificate, accessibili solo a chi ne ha necessità e conservate secondo il calendario applicabile. Hash e revisione documentale identificano i documenti, ma non provano da soli l'efficacia di un controllo.

La verifica valuta esistenza, pertinenza, copertura, data, risultato e limiti dell'evidenza. Campioni e test devono essere rappresentativi del rischio dichiarato. Esiti negativi o parziali generano un'azione con owner e scadenza; non sono omessi dalla sintesi quando incidono sulla comprensione del rischio.

- registro revisioni documentali, approvazioni e distribuzione
- matrice di applicabilità con owner, motivazione e stato
- verbali di riesame e piano delle azioni correttive
- registro eccezioni con scadenza e misure compensative
- collegamenti a contratti, procedure e prove tecniche

Salvaguardie trasversali

Privacy, sicurezza, qualità e continuità sono considerate in ogni fase e non soltanto al termine. I dati sono limitati a quanto necessario; accessi e autorizzazioni seguono il minimo privilegio; modifiche e attività amministrative sono tracciate in misura proporzionata; input, trasformazioni e output mantengono una provenienza sufficiente alla verifica professionale.

Dati particolari, informazioni altamente riservate, minori o persone vulnerabili richiedono una valutazione specifica prima del trattamento. Quando il controllo necessario non è disponibile o non è provato, si riduce il perimetro, si applica una modalità manuale, si rimuove il dato o si sospende il caso d'uso.

- minimizzazione di dati, campi liberi, prompt, log ed export
- accesso nominativo, segregazione dei ruoli e revoca tempestiva
- validazione di formato, integrità, completezza e provenienza
- protezione di trasporto, copie di lavoro e canali di condivisione secondo evidenza
- modalità degradata, escalation e comunicazione quando dipendenze o controlli non sono disponibili

Eccezioni, non conformità ed escalation

Uno scostamento non è accettato per consuetudine. L'owner registra requisito interessato, causa, impatto, dati e persone esposte, misure compensative, approvatore, scadenza e criterio di chiusura. L'eccezione è riesaminata se cambia il rischio o se una misura non produce l'effetto previsto.

Devono essere escalati senza ritardo incidenti, possibile trattamento illecito, perdita di controllo sui dati, output con impatto grave, violazioni contrattuali, fornitore non approvato o evidenza inattendibile. Ai fini del presente documento si considera quanto segue: I servizi di pagamento non rientrano nel perimetro descritto dalla presente documentazione.

- contenere il rischio e sospendere la fase interessata quando necessario
- preservare prove, orari, decisioni e comunicazioni
- coinvolgere owner privacy, sicurezza, prodotto, legale o direzione secondo il caso
- riattivare solo dopo verifica della misura e autorizzazione documentata

Riesame, modifiche e miglioramento

Il documento è riesaminato almeno semestralmente e prima quando cambiano finalità, destinatari, dati, ruolo GDPR o AI Act, provider, modello, architettura, localizzazione, termini contrattuali o requisiti normativi. Incidenti, reclami, test falliti e nuove vulnerabilità attivano un riesame straordinario.



Ogni revisione registra input, partecipanti, decisione, modifiche, evidenze sostituite, gap residui e data successiva. Correzioni materiali sono pubblicate senza alterare retroattivamente la revisione documentale precedente. Contatti e richieste: info@nil-tech.net.

- verifica del registro modifiche e dei documenti collegati
- nuovo test dei controlli interessati
- aggiornamento di manifest, PDF, HTML e hash
- comunicazione ai destinatari quando la modifica incide sui loro diritti o obblighi

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 2026-07-27. 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) e quadro della Commissione
- Regolamento (UE) 2022/2554 (DORA)
- Regolamento (UE) 2023/2854 (Data Act)
- Direttiva (UE) 2022/2555 (NIS2) e stato di attuazione in Italia
- Regolamento (UE) 2024/2847 (Cyber Resilience Act)

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.