SECURITY & COMPLIANCE

Politica per un’intelligenza artificiale responsabile e trasparenza AI Act

Uso previsto, trasparenza, alfabetizzazione e governo degli output IA.

Prodotto	ClaimEvidence
Codice	CLE-PUB-13-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 definire principi e controlli per un uso dell'IA lecito, trasparente, proporzionato, sorvegliabile e coerente con il caso d'uso.

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 politica applica un approccio fondato sul rischio e sui diritti fondamentali, coerente con il Regolamento (UE) 2024/1689. Ruolo nella catena del valore, classificazione e obblighi sono determinati con riferimento al singolo sistema e al relativo uso previsto, senza classificazioni generalizzate.

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 inventariare sistemi, modelli, provider, revisioni documentali e owner. 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 valutare uso previsto, uso improprio, persone esposte e impatti. 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 limitare dati e prompt e prevenire divulgazioni non necessarie. 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 informare utenti su natura assistita, capacità e limitazioni. 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 rendere possibile verifica, override, stop ed escalation. 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 monitorare qualità, bias, incidenti e cambiamenti materiali. Owner, perimetro, dipendenze, criterio di accettazione ed evidenza sono identificati nel fascicolo applicabile; in loro assenza il presidio non è considerato dimostrato.

Uso dell’IA

L’IA può assistere interpretazione e segnali di flusso; non determina copertura, responsabilità o liquidazione. Il responsabile autorizzato verifica evidenze e output prima della decisione.

L’IA può assistere interpretazione e segnali di flusso; non determina copertura, responsabilità o liquidazione. Il responsabile autorizzato verifica evidenze e output prima della decisione.

Trasparenza

Gli utenti devono sapere quando interagiscono con funzioni IA o ricevono contenuti assistiti. Output destinati a comunicazione esterna devono essere verificati e identificati quando la legge o il contesto lo richiedono.

Governance

- inventario di sistemi, modelli, ruoli, revisioni documentali e finalità
- classificazione d’uso e rischio basata sul contesto, non sul solo prodotto
- valutazione di dati, accuratezza, robustezza, sicurezza e diritti
- alfabetizzazione IA e istruzioni per gli operatori
- monitoraggio, incidenti, reclami e riesame

Stato normativo

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.

Non è attribuita una classe di rischio definitiva senza esame dello specifico uso del cliente e delle modifiche normative applicabili.

Ruolo nella catena del valore e classificazione

La qualifica di fornitore, deployer, importatore o distributore ai sensi dell'AI Act è determinata per ciascun sistema e caso d'uso, considerando chi sviluppa o fa sviluppare, immette sul mercato con il proprio nome, modifica sostanzialmente o determina la finalità. L'uso di un modello di terzi non rende automaticamente Niltech mero deployer né automaticamente fornitore del modello generale.

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.

La classificazione è riaperta quando cambiano finalità prevista, utenti, persone incise, modello, dati, grado di autonomia, integrazione in un prodotto regolato o uso da parte di un'autorità. Non sono utilizzate etichette generiche come "rischio limitato" quale conclusione definitiva.

Trasparenza, alfabetizzazione e contenuti generati

Niltech adotta misure per sostenere l'alfabetizzazione in materia di IA del personale e delle persone che operano i sistemi per suo conto, calibrate su conoscenze, esperienza, contesto e soggetti incisi. L'articolo 4, come modificato dal Regolamento (UE) 2026/1744, non impone di garantire a ciascuna persona uno specifico livello, ma richiede misure effettive e dimostrabili.

Dal 2 agosto 2026 l'articolo 50 è applicabile e richiede, nei casi pertinenti, informazione chiara quando una persona interagisce direttamente con un sistema IA e marcatura in formato leggibile meccanicamente e rilevabile dei contenuti sintetici; i deployer devono inoltre etichettare deepfake e taluni testi di interesse pubblico non sottoposti a revisione umana o controllo editoriale. La modalità concreta tiene conto delle linee guida finali della Commissione pubblicate nel luglio 2026 e non è sostituita da una clausola nascosta nei termini.

I sistemi che generano contenuti sintetici e sono stati immessi sul mercato prima del 2 agosto 2026 beneficiano, per l'obbligo di marcatura dell'articolo 50, paragrafo 2, del termine transitorio previsto al 2 dicembre 2026. Tale termine non sospende gli altri obblighi applicabili.

Principi di impiego

- finalità determinata, dati pertinenti, provenienza verificabile e divieto di pratiche vietate
- informazione comprensibile su natura dell'assistenza, limiti e controllo umano
- test proporzionati su accuratezza, robustezza, bias, sicurezza e usi impropri ragionevolmente prevedibili
- possibilità effettiva di contestare, correggere, ignorare, sospendere ed escalare l'output

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) 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
- Commissione europea — Alfabetizzazione in materia di IA dopo il Regolamento (UE) 2026/1744
- Regolamento (UE) 2016/679 (GDPR)

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.