SECURITY & COMPLIANCE

Panoramica sicurezza, architettura e misure tecniche e organizzative

Architettura, responsabilità condivise e misure verificabili.

Prodotto	Andrea AI
Codice	AND-PUB-09-IT
Edizione documentale	Edizione del 29 luglio 2026
Efficacia / riesame	2026-07-29 / 2027-01-29
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 Calmaggiore 5, 31100 Treviso (TV), Italia, P. IVA IT 05614380268 (di seguito «Niltech»), adotta il presente documento al fine di presentare un quadro comprensibile dell'architettura e delle misure senza confondere capacità del provider, configurazioni Niltech ed evidenze disponibili.

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.

Le misure descritte costituiscono un quadro di governance ai sensi degli articoli 24, 25 e 32 GDPR. Adeguatezza ed efficacia devono essere valutate in relazione a natura, oggetto, contesto, finalità e rischio del singolo trattamento; nessuna misura è qualificata come assoluta.

Ambito soggettivo e oggettivo

Il perimetro oggettivo comprende Andrea AI, le relative interfacce pubbliche e i trattamenti strettamente connessi alle funzionalità descritte. Il sito commerciale e la libreria documentale sono pubblicati su andreaaiagent.com e utilizzano infrastruttura Bluehost, MySQL e il trasporto di posta del server. L’applicazione è resa disponibile sul distinto dominio andreaai.net mediante infrastruttura Hetzner; Pinecone, Cloudflare, OpenAI e Google Gemini intervengono nei limiti delle funzioni e degli accordi applicabili.

Le operazioni considerate riguardano acquisizione e analisi di documenti e immagini, supporto alla lettura di polizze, stime e bozze di relazione, organizzazione del fascicolo e indicatori ESG solo quando fondati su dati verificabili. Le categorie di informazioni potenzialmente interessate sono: dati di contatto e prospect sul sito; nell’applicazione, dati di pratica, documenti, immagini, note, metadati tecnici e output assistiti dall’IA secondo configurazione e contratto. 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 Andrea AI 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 mantenere inventario, classificazione e owner di asset e dati. 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 applicare accessi nominativi, minimo privilegio e riesame periodico. 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 gestire configurazioni, segreti e modifiche con segregazione e tracciabilità. 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 raccogliere log e alert proporzionati, protetti da alterazione e abuso. 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 gestire vulnerabilità, dipendenze, patch e accettazioni del rischio. 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 provare risposta incidenti, backup, ripristino e continuità. Owner, perimetro, dipendenze, criterio di accettazione ed evidenza sono identificati nel fascicolo applicabile; in loro assenza il presidio non è considerato dimostrato.

Perimetro e architettura

Il sito commerciale e la libreria documentale sono pubblicati su andreaaiagent.com e utilizzano infrastruttura Bluehost, MySQL e il trasporto di posta del server. L’applicazione è resa disponibile sul distinto dominio andreaai.net mediante infrastruttura Hetzner; Pinecone, Cloudflare, OpenAI e Google Gemini intervengono nei limiti delle funzioni e degli accordi applicabili.

Catena tecnologica rilevante: Bluehost, Hetzner, Pinecone, Cloudflare, OpenAI, Google Gemini, MySQL, Exim/sendmail.

Misure organizzative

- accessi nominativi e principio del minimo privilegio
- gestione di modifiche, incidenti, fornitori e diritti
- formazione e revisione periodica proporzionate ai ruoli
- classificazione dei documenti e condivisione controllata delle prove

Misure tecniche

Autenticazione, autorizzazione, protezione del trasporto, logging, isolamento ambienti, aggiornamenti, gestione segreti, backup e monitoraggio sono applicati secondo il componente e verificati tramite evidenze. Questo documento non dichiara algoritmi, certificazioni o configurazioni non documentate.

Responsabilità condivisa

Niltech gestisce applicazione e configurazioni sotto il proprio controllo; i provider gestiscono le rispettive piattaforme; il cliente gestisce utenti, finalità, dati, dispositivi e decisioni. I confini contrattuali prevalgono.

Criterio di adeguatezza delle misure

Le misure sono selezionate considerando probabilità e gravità per diritti, continuità e patrimonio informativo, stato dell'arte, costi e dipendenze. La presente panoramica non attesta che ogni misura sia applicata allo stesso modo a ogni componente: il fascicolo controllato associa controllo, ambito, owner, prova, risultato del test, eccezione e data di riesame.

Non sono dichiarati algoritmi, lunghezze di chiave, certificazioni, regioni, obiettivi di ripristino o frequenze non provati. La cifratura, il logging, il backup o la scansione automatica riducono rischi specifici ma non eliminano errori di configurazione, abuso di privilegi, dipendenze o indisponibilità.

Responsabilità condivisa e accesso alle evidenze

Niltech governa i componenti sotto il proprio controllo; il fornitore risponde dei propri servizi secondo contratto; il Cliente governa utenze, istruzioni, terminali, destinatari, basi giuridiche e corretto impiego degli output. Una carenza del Cliente non esonera Niltech dai propri obblighi e viceversa.

Diagrammi dettagliati, configurazioni, report di vulnerabilità, evidenze di accesso e procedure di risposta sono riservati e forniti, quando giustificato, mediante security pack controllato, accordo di riservatezza o diritto di audit. La limitazione tutela la sicurezza e non può essere usata per sottrarre informazioni necessarie al titolare o all'autorità.

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 Andrea AI 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 2026-07-29. L'applicabilità, il ruolo e le eventuali decorrenze devono essere nuovamente accertati sul caso concreto.

- Regolamento (UE) 2016/679 (GDPR)

- 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