SECURITY & COMPLIANCE

Responsible artificial intelligence policy and AI Act transparency

Intended use, transparency, literacy and governance of AI outputs.

Product	ClaimEvidence
Code	CLE-PUB-13-EN
Document edition	Edition dated 30 August 2026
Effective / review	2026-08-30 / 2027-02-28
Document owner	Nil Tech Europe S.r.l. · Compliance & Security
Classification	Public

Preamble, nature and effect of this document

Nil Tech Europe S.r.l., with registered office at Via Calmaggiore 5, 31100 Treviso (TV), Italia, VAT No. IT 05614380268 (“Niltech”), adopts this document in order to define principles and controls for lawful, transparent, proportionate and overseen AI use consistent with the use case.

This document is a corporate transparency and accountability record. It is not a third-party certification, legal opinion addressed to persons other than the company, absolute security warranty or blanket compliance statement; contractual commitments arise solely from the applicable agreements.

This policy applies a risk- and fundamental-rights-based approach consistent with Regulation (EU) 2024/1689. Value-chain role, classification and duties are determined by reference to each system and its intended purpose, without blanket classifications.

Personal and material scope

The objective scope includes ClaimEvidence, its public interfaces and processing strictly connected with the described functions. The corporate website and document library are published on claimevidence.tech; the application service is available through the separate app.claimevidence.tech domain. Hostinger provides infrastructure and, according to the applicable configuration, mail transport. MySQL/MariaDB is software running in the controlled environment and not a separate subprocessor unless a distinct managed service is used. OpenAI provides API services only for enabled functions; any separate email provider must be identified and assessed before use.

The relevant operations concern guided photo and document collection, case organisation, completeness checks, configurable analytical support, human review and export. Potential information categories are: demo and security-pack requests on the site; in the application, case identifiers, authorised contacts, photographs, documents, notes, session metadata and assisted outputs. The actual privacy role, lawful basis and extent of processing depend on the contractual relationship and the lawful instructions of the party determining purposes and essential means.

Definitions and interpretation

- “Service” means the ClaimEvidence functions made available under the agreement.
- “Customer” means the legal person or professional entering into the agreement with Niltech.
- “Authorised User” means an individual enabled by the Customer to use the Service under its responsibility.
- “Customer Data” means data, documents, images, instructions and other content submitted or generated on the Customer’s behalf.

- “Assisted Output” means a result produced through automated rules or artificial-intelligence components and subject to the stated controls.
- “Further Supplier” means a third party providing Niltech with a technical service relevant to the documented scope.
- “Incident” means an event compromising or capable of compromising confidentiality, integrity, availability, authenticity or resilience.
- “Business Day” means a day other than Saturday, Sunday or an Italian national public holiday.

Specific duties and safeguards

1. Within its assigned role and without prejudice to the Customer’s responsibilities, Niltech shall inventory systems, models, providers, document revisions and owners. The applicable file identifies the owner, scope, dependencies, acceptance criterion and evidence; absent those elements, the safeguard is not treated as demonstrated.

2. Within its assigned role and without prejudice to the Customer’s responsibilities, Niltech shall assess intended use, misuse, exposed persons and impacts. The applicable file identifies the owner, scope, dependencies, acceptance criterion and evidence; absent those elements, the safeguard is not treated as demonstrated.

3. Within its assigned role and without prejudice to the Customer’s responsibilities, Niltech shall minimise data and prompts and prevent unnecessary disclosure. The applicable file identifies the owner, scope, dependencies, acceptance criterion and evidence; absent those elements, the safeguard is not treated as demonstrated.

4. Within its assigned role and without prejudice to the Customer’s responsibilities, Niltech shall inform users about assisted nature, capabilities and limitations. The applicable file identifies the owner, scope, dependencies, acceptance criterion and evidence; absent those elements, the safeguard is not treated as demonstrated.

5. Within its assigned role and without prejudice to the Customer’s responsibilities, Niltech shall enable review, override, stop and escalation. The applicable file identifies the owner, scope, dependencies, acceptance criterion and evidence; absent those elements, the safeguard is not treated as demonstrated.

6. Within its assigned role and without prejudice to the Customer’s responsibilities, Niltech shall monitor quality, bias, incidents and material changes. The applicable file identifies the owner, scope, dependencies, acceptance criterion and evidence; absent those elements, the safeguard is not treated as demonstrated.

Use of AI

AI may assist interpretation and workflow signals; it does not determine coverage, liability or settlement. The authorised reviewer verifies evidence and outputs before a decision.

AI may assist interpretation and workflow signals; it does not determine coverage, liability or settlement. The authorised reviewer verifies evidence and outputs before a decision.

Transparency

Users must know when they interact with AI functions or receive assisted content. Outputs intended for external communication must be reviewed and identified where law or context requires.

Governance

- inventory of systems, models, roles, document revisions and purposes
- context-based use and risk classification, not product-only
- assessment of data, accuracy, robustness, security and rights
- AI literacy and operator instructions
- monitoring, incidents, complaints and review

Regulatory status

Concrete applicability depends on Niltech’s role, the customer, sector, intended use, data categories and configuration. Conclusions are reviewed whenever one of those elements changes.

No final risk class is assigned without review of the customer's specific use and applicable regulatory changes.

Scope, audience and status of this document

This document is intended for customers, prospects, authorised users, advisers and control functions needing to understand the ClaimEvidence scope. Its specific objective is to define principles and controls for lawful, transparent, proportionate and overseen AI use consistent with the use case. It applies to the stated document revision and date and must be read with the applicable agreement, order, DPA, technical specifications and controlled procedures.

The corporate website and document library are published on claimevidence.tech; the application service is available through the separate app.claimevidence.tech domain. Hostinger provides infrastructure and, according to the applicable configuration, mail transport. MySQL/MariaDB is software running in the controlled environment and not a separate subprocessor unless a distinct managed service is used. OpenAI provides API services only for enabled functions; any separate email provider must be identified and assessed before use.

Executed agreements and actually approved configurations prevail in case of inconsistency. Public information describes the control programme; it does not turn optional provider capabilities into Niltech controls or automatically attest legal applicability or satisfaction.

Exceptions, non-conformity and escalation

A deviation is not accepted by custom. The owner records the affected requirement, cause, impact, exposed data and persons, compensating measures, approver, expiry and closure criterion. The exception is reviewed if risk changes or a measure does not work as expected.

Incidents, possible unlawful processing, loss of data control, outputs with severe impact, contractual breaches, unapproved suppliers or unreliable evidence must be escalated without delay. Current Legal and functional scope: Payment services are outside the scope described by this documentation.

- contain risk and suspend the affected phase where needed
- preserve evidence, timing, decisions and communications
- involve privacy, security, product, legal or management owners as appropriate
- resume only after measure verification and documented authorisation

Review, change and improvement

The document is reviewed at least every six months and earlier when purpose, audience, data, GDPR or AI Act role, supplier, model, architecture, location, contractual terms or legal requirements change. Incidents, complaints, failed tests and new vulnerabilities trigger an extraordinary review.

Each review records inputs, participants, decision, changes, superseded evidence, remaining gaps and next date. Material corrections are published without retroactively altering the prior document revision. Contact and requests: info@nil-tech.net.

- check change register and related documents
- retest affected controls
- update manifest, PDF, HTML and hashes
- notify recipients where the change affects their rights or duties

Value-chain role and classification

Provider, deployer, importer or distributor status under the AI Act is determined for each system and use case, considering who develops or has it developed, places it on the market under its name, substantially modifies it or determines its purpose. Using a third-party model does not automatically make Niltech merely a deployer or automatically the provider of the general-purpose model.

Collecting and organising claim evidence and supporting review do not, as such, determine coverage, liability or settlement and are not abstractly classified as a high-risk use. Classification must be reopened if the system is intended to decide or autonomously recommend outcomes producing legal or similarly significant effects.

Classification is reopened when intended purpose, users, affected persons, model, data, autonomy, integration into a regulated product or use by an authority changes. Generic labels such as “limited risk” are not used as a definitive conclusion.

Transparency, literacy and generated content

Niltech takes measures supporting AI literacy of staff and persons operating systems on its behalf, calibrated to knowledge, experience, context and affected persons. Article 4, as amended by Regulation (EU) 2026/1744, does not require a particular level to be guaranteed for each individual but does require effective and demonstrable measures.

Article 50 has applied since 2 August 2026 and requires, where relevant, clear notice when a person directly interacts with an AI system and machine-readable, detectable marking of synthetic content; deployers must also label deepfakes and certain public-interest text lacking human review or editorial control. The concrete method reflects the Commission’s final guidelines published in July 2026 and is not replaced by a clause hidden in terms.

Systems generating synthetic content and placed on the market before 2 August 2026 benefit, for the Article 50(2) marking duty, from the transitional deadline of 2 December 2026. That deadline does not suspend other applicable duties.

Use principles

- specified purpose, relevant data, verifiable provenance and prohibition of banned practices
- intelligible information about the nature of assistance, limitations and human control
- proportionate testing for accuracy, robustness, bias, security and reasonably foreseeable misuse
- effective ability to challenge, correct, disregard, suspend and escalate outputs

Allocation of responsibility and reliance limitations

Within its sphere of responsibility, the Customer warrants the lawfulness of submitted data and instructions, user authorisation, suitable lawful bases and notices, and professional verification of outputs. Niltech remains responsible for activities directly under its control and does not assume the Customer’s regulatory, professional or decision-making functions.

Outputs from ClaimEvidence are auxiliary. Unless expressly agreed and subject to mandatory law, they are not legal advice, an expert determination, insurance decision, liability finding, credit assessment or other reserved professional act. The recipient must examine sources, completeness, consistency and consequences before use.

Nothing excludes liability that cannot lawfully be excluded. Outside those cases, attribution, remedies, limitations and quantification principles follow the applicable agreement, taking account of contributory conduct, mitigation duties and foreseeability under the governing law.

Evidence, review, requests and governing law

Every material assertion must be traceable to a contract, approved configuration, register, minutes, test, log or other reliable evidence. Supplier statements and Niltech controls are kept distinct. Absence of incidents is not, by itself, proof that a measure is effective.

Revisions are dated, reasoned and approved. A later revision does not retroactively alter facts or commitments applicable to earlier periods. Published copies are identified by code, date and cryptographic digest; those elements evidence copy integrity, not the substantive effectiveness of described controls.

Reports, clarification requests, rights requests and complaints may be sent to info@nil-tech.net. Niltech verifies identity and authority where necessary, records the request, responds within applicable periods and communicates any reasoned extension or refusal.

Unless mandatory law or a written agreement provides otherwise, Italian law governs interpretation. The Italian text is controlling; the English translation is provided for convenience.

Official sources and legal date

References checked on 2026-08-30. Applicability, role and any relevant commencement dates must be reassessed against the concrete facts.

- Regulation (EU) 2024/1689 (AI Act)
- Regulation (EU) 2026/1744 — Digital Omnibus on AI
- European Commission — Final guidelines on Article 50 AI Act transparency obligations, July 2026
- European Commission — AI literacy following Regulation (EU) 2026/1744
- Regulation (EU) 2016/679 (GDPR)