SECURITY & COMPLIANCE

Product privacy notice and GDPR roles

Roles, data categories and GDPR responsibilities in the service.

Product	ClaimEvidence
Code	CLE-PUB-03-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 transparently describe GDPR roles, product data, customer instructions and responsibilities that remain separate.

This document is a notice provided to data subjects. Consent is not required where processing relies on another lawful basis; where consent is necessary, it is requested separately in a freely given, specific, informed and withdrawable manner.

This document applies the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability under Articles 5, 24, 25 and 32 GDPR, while keeping the customer’s position distinct from Niltech’s position.

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 define by contract when Niltech is processor and when it acts as independent controller. 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 document data subjects, data, sources, purposes and operations. 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 apply minimisation to uploads, prompts, logs, support and exports. 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 restrict access to users and staff with documented need. 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 assist the controller with rights, DPIA, incidents and consultations. 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 cease, return or delete data according to instructions and applicable constraints. The applicable file identifies the owner, scope, dependencies, acceptance criterion and evidence; absent those elements, the safeguard is not treated as demonstrated.

Roles

The customer normally acts as controller for data entered into the product; Niltech generally operates as processor on documented instructions. Niltech remains controller for accounts, security, billing, compliance and its own contacts.

Data and data subjects

demo and security-pack requests on the site; in the application, case identifiers, authorised contacts, photographs, documents, notes, session metadata and assisted outputs

Data subjects may include users, end customers, insured parties, counterparties, advisers or persons mentioned in documents. The customer must limit data to necessity and provide a lawful basis and notices.

Purposes and instructions

ClaimEvidence supports guided photo and document collection, case organisation, completeness checks, configurable analytical support, human review and export.

Niltech does not use customer data for purposes incompatible with the contract. Any further use requires a separate basis and notice.

Rights and assistance

Requests concerning product data normally go to the customer controller. Niltech assists with search, export, restriction, rectification and deletion within the service and DPA.

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 transparently describe GDPR roles, product data, customer instructions and responsibilities that remain separate. 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

Allocation of roles and own purposes

For content submitted by the Customer, the Customer ordinarily determines purposes and essential means and acts as controller; Niltech processes on its behalf under Article 28 GDPR. Classification nevertheless depends on facts, not the contractual label. If two parties jointly determine purposes and essential means, an Article 26 arrangement is required; if Niltech independently determines a further purpose, it acts as controller for that processing and must provide a separate notice.

Niltech normally acts as controller for account and contract administration, security of its service, abuse prevention, establishment or defence of claims, accounting duties and compliance requests. Those purposes do not authorise reuse of Customer content to train general models or for incompatible purposes.

Case photographs, documents and metadata may reveal faces, vehicle-registration numbers, locations, health conditions, minors or persons unrelated to the case. The Customer must establish collection instructions that avoid excessive capture, redact unnecessary elements where reasonably possible and document any applicable Article 9 and 10 GDPR conditions.

Customer obligations and safeguards for individuals

Before submission, the Customer must identify purposes, lawful basis, data-subject categories, retention periods and authorised persons; provide required notices; manage objections, restrictions and other rights; carry out a DPIA or prior consultation where required; and issue lawful documented instructions.

Niltech forwards to the Customer requests received concerning data processed on its behalf and does not answer substantively unless authorised or legally required. Assistance reflects the nature of processing and information available, without collecting unnecessary additional data.

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) 2016/679 (GDPR)
- EDPB — Guidelines 07/2020 on controller and processor concepts

Document control: the copy identified in the manifest through its SHA-256 digest is the document edition published on the stated date. The header seal is neutral corporate artwork and is not a digital signature, third-party attestation or certification.