SECURITY & COMPLIANCE

DORA-oriented ICT supplier information sheet

Information for ICT due diligence by DORA-regulated customers.

Product	ClaimEvidence
Code	CLE-PUB-18-EN
Document edition	Edition dated 27 July 2026
Effective / review	2026-07-27 / 2027-01-27
Document owner	Niltech Europe S.r.l. · Compliance & Security
Classification	Public

Preamble, nature and effect of this document

Niltech 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 provide financial customers with ICT due-diligence information without attributing unverified duties or qualifications to Niltech.

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 sheet supports due diligence by customers subject to Regulation (EU) 2022/2554. It does not qualify Niltech as a financial entity or replace mandatory clauses, the register of information or the customer's own assessment.

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 infrastructure, the relational database, mail transport and OpenAI APIs operate according to their respective functions and contractual terms.

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 describe service, supported functions, dependencies and contractual locations. Performance is governed by necessity, proportionality and traceability, assigned to an accountable person and supported by evidence appropriate to the nature of the risk. Where performance depends on information, authorisation or action by the Customer or a supplier, that dependency is communicated and recorded; absence of the required condition prevents the control from being treated as fully operational.

2. Within its assigned role and without prejudice to the Customer's responsibilities, Niltech shall state security, incident, continuity and subcontracting governance. Performance is governed by necessity, proportionality and traceability, assigned to an accountable person and supported by evidence appropriate to the nature of the risk. Where performance depends on information, authorisation or action by the Customer or a supplier, that dependency is communicated and recorded; absence of the required condition prevents the control from being treated as fully operational.

3. Within its assigned role and without prejudice to the Customer's responsibilities, Niltech shall support customer criticality and concentration classification. Performance is governed by necessity, proportionality and traceability, assigned to an accountable person and supported by evidence appropriate to the nature of the risk. Where performance depends on information, authorisation or action by the Customer or a supplier, that dependency is communicated and recorded; absence of the required condition prevents the control from being treated as fully operational.

4. Within its assigned role and without prejudice to the Customer's responsibilities, Niltech shall map notice, cooperation, audit and access requirements. Performance is governed by necessity, proportionality and traceability, assigned to an accountable person and supported by evidence appropriate to the nature of the risk. Where performance depends on information, authorisation or action by the Customer or a supplier, that dependency is communicated and recorded; absence of the required condition prevents the control from being treated as fully operational.

5. Within its assigned role and without prejudice to the Customer's responsibilities, Niltech shall define portability, transition assistance and termination. Performance is governed by necessity, proportionality and traceability, assigned to an accountable person and supported by evidence appropriate to the nature of the risk. Where performance depends on information, authorisation or action by the Customer or a supplier, that dependency is communicated and recorded; absence of the required condition prevents the control from being treated as fully operational.

6. Within its assigned role and without prejudice to the Customer's responsibilities, Niltech shall manage restricted evidence with proportionate non-destructive access. Performance is governed by necessity, proportionality and traceability, assigned to an accountable person and supported by evidence appropriate to the nature of the risk. Where performance depends on information, authorisation or action by the Customer or a supplier, that dependency is communicated and recorded; absence of the required condition prevents the control from being treated as fully operational.

Role in the ICT chain

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

The corporate website and document library are published on claimevidence.tech. The application service is available through the separate app.claimevidence.tech domain. Hostinger infrastructure, the relational database, mail transport and OpenAI APIs operate according to their respective functions and contractual terms.

Available information

- services, data, environments, contractual locations and subcontractors
- contacts, incidents, continuity, audit and exit under contract
- dependencies and concentration to be assessed by the customer

Customer responsibility

The financial customer remains responsible for its assessment, information register, function classification, contractual requirements, testing and exit strategy. This document does not qualify Niltech as certified or compliant on the customer's behalf.

Controlled evidence

DPA, supplier register, incident procedures, continuity, tests, assessments and limitations are available through a controlled process and confidentiality arrangements.

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 provide financial customers with ICT due-diligence information without attributing unverified duties or qualifications to Niltech. 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 infrastructure, the relational database, mail transport and OpenAI APIs operate according to their respective functions and contractual terms.

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.

Operational definitions

The following definitions support consistent interpretation. Terms defined by law or contract retain the meaning assigned by the relevant source.

- Critical service: function whose unavailability causes a material customer impact.
- Continuity: organisational ability to maintain or restore priority activities during an event.
- Backup: protected copy intended for restoration and distinct from replication or high availability.
- Restore: controlled recovery of data and services followed by integrity and functional checks.
- Scenario: plausible event used to plan response, communications, resources and dependencies.

Requirements and operating process

The process must remain proportionate to the use case, data, exposed persons and possible impact. Relevant ClaimEvidence functions include guided photo and document collection, case organisation, completeness checks, configurable analytical support, human review and export. Every phase must have an owner, verifiable inputs, completion criteria, evidence and an escalation path.

Before activation or publication, the owner verifies that requirements are translated into concrete controls and that controls actually apply to the environment. A merely planned control, an unconfigured capability or a general supplier statement is recorded as a gap, not as an operating measure.

- describe service, supported functions, dependencies and contractual locations
- state security, incident, continuity and subcontracting governance
- support customer criticality and concentration classification
- map notice, cooperation, audit and access requirements
- define portability, transition assistance and termination
- manage restricted evidence with proportionate non-destructive access

Roles and responsibilities

Niltech maintains this document, configurations under its control and links to evidence. The customer determines purposes, users, data, authorisations and professional decisions within its scope. Providers are responsible for components defined by their contracts. The primary product audience is firms, adjusters and organisations collecting and reviewing claim evidence.

No role is assigned implicitly. Product, security, privacy, continuity and AI owners must be identified in the controlled register. Where one person performs multiple roles, material risk, exception or result approval must include proportionate independent review.

- Management: approves residual risk, material exceptions and priorities.
- Owner: maintains requirements, controls, evidence, gaps and reviews.
- Operators: follow instructions, verify inputs/outputs and report anomalies.
- Customer: ensures lawfulness, authorisations, data quality and professional use.
- Suppliers: provide services and information under their agreements.

Evidence, verification and accountability

Every material statement must trace to current evidence: configuration, contract, report, test, ticket, minutes, log or register. Evidence is classified, restricted to those with a need and retained under the applicable schedule. Hash and document revision identify documents but do not alone prove control effectiveness.

Verification assesses evidence existence, relevance, coverage, date, result and limitations. Samples and tests must represent the stated risk. Negative or partial results create an action with owner and due date; they are not omitted from the summary where they affect risk understanding.

- business impact analysis and dependency inventory
- continuity, communication and recovery plans
- backup inventory and isolated restore evidence
- scenario tests, results, gaps and remediation
- incidents, activation decisions and lessons learned

Cross-cutting safeguards

Privacy, security, quality and continuity are considered at every phase, not only at completion. Data is limited to what is necessary; access and authorisation follow least privilege; changes and administrative activity are traced proportionately; inputs, transformations and outputs retain provenance sufficient for professional review.

Special-category data, highly confidential information, minors or vulnerable persons require a specific assessment before processing. Where a required control is unavailable or unproven, scope is reduced, a manual mode is used, the data is removed or the use case is suspended.

- minimisation of data, free-text fields, prompts, logs and exports
- named access, role segregation and timely revocation
- format, integrity, completeness and provenance validation
- evidence-based protection of transport, working copies and sharing channels
- degraded mode, escalation and communication where dependencies or controls are unavailable

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 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 2026-07-27. Applicability, role and any relevant commencement dates must be reassessed against the concrete facts.

• Regulation (EU) 2022/2554 (DORA)

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.