SECURITY & COMPLIANCE

Regulatory applicability and compliance-controls matrix

Dated matrix of applicability, responsibilities and required evidence.

Product	ClaimEvidence
Code	CLE-PUB-24-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 maintain a reasoned assessment of applicability, role, requirements, evidence, gaps and actions for major regulatory frameworks.

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.

The matrix is a requirement-identification and governance tool, not a formal legal opinion or blanket compliance attestation. Applicability, role, duties and dates are verified against the concrete facts and current official sources.

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 analyse entity, sector, size, territory, role and use case. 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 separate direct, contractual, supply-chain and good-practice duties. 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 link each requirement to an owner, control and evidence. 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 record gap, risk, priority, due date and dependencies. 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 verify official sources and application dates. 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 review after legal, contractual or technical changes. The applicable file identifies the owner, scope, dependencies, acceptance criterion and evidence; absent those elements, the safeguard is not treated as demonstrated.

Method

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.

The matrix is a readiness tool, not legal advice or a blanket compliance declaration.

Matrix

Framework	Assessment	Evidence / actions
GDPR	Applies to personal-data processing; roles vary.	DPA, ROPA, DPIA, rights, security, suppliers.
AI Act	Applicability and class depend on intended use and value-chain role.	Inventory, assessment, transparency, oversight, literacy.
DORA	Directly for financial customers; contractual and due-diligence requirements may flow to the ICT supplier.	Supplier sheet, incidents, continuity, audit, exit.
Data Act	Assess for portability, switching and data terms.	Export, exit, data catalogue, contract.
NIS2	Assess by sector, size, role and supply chain.	Risk management, incidents, continuity, suppliers.
CRA	Assess against qualification as a product with digital elements and role.	Secure development, vulnerabilities, updates, reporting.

Legal and functional scope

Payment services are outside the scope described by this documentation.

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.

Review

Review every six months and after relevant changes to law, role, use, data, provider, architecture or incident. Actions and evidence are in the controlled register.

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 maintain a reasoned assessment of applicability, role, requirements, evidence, gaps and actions for major regulatory frameworks. 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

Applicability method

For each source, the matrix identifies obligated person, subject matter, territory, role, threshold or classification, duty, commencement date, evidence, owner and reasoned conclusion. “Applicable”, “not applicable”, “indirectly relevant” and “to be determined” are not interchangeable, and the conclusion is reopened when facts change.

Voluntary adoption of a safeguard drawn from a law does not prove that the law applies or that all its requirements are met. Likewise, absence from direct scope does not remove contractual or supply-chain duties.

Verified legal timeline

- GDPR: applicable since 25 May 2018; roles and duties depend on concrete processing
- DORA: applicable since 17 January 2025 to entities and ICT relationships within scope
- Data Act: applicable since 12 September 2025, subject to specific commencement rules and exceptions
- NIS2 in Italy: transposed by Legislative Decree No. 138 of 4 September 2024; applicability depends on entity, sector and service
- AI Act: duties and prohibitions have different commencement dates; Article 50 transparency applicable since 2 August 2026; Annex III high-risk systems from 2 December 2027 and Annex I systems from 2 August 2028, as amended by Regulation (EU) 2026/1744
- Cyber Resilience Act: conformity-assessment-body provisions applicable since 11 June 2026, reporting duties from 11 September 2026 and main duties from 11 December 2027, subject to scope assessment

AI use-case outcome

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.

The outcome does not remove otherwise applicable duties, including transparency, literacy, data protection, security, consumer protection and professional fairness. Each new purpose undergoes change assessment before use.

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)
- 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
- Regulation (EU) 2022/2554 (DORA)
- Regulation (EU) 2023/2854 (Data Act)
- Directive (EU) 2022/2555 (NIS2)
- Italian Legislative Decree No. 138 of 4 September 2024 — NIS2 implementation
- Regulation (EU) 2024/2847 (Cyber Resilience Act)
- European Commission — Cyber Resilience Act implementation framework and dates, 27 July 2026