



SECURITY & COMPLIANCE

AI system card and legal-operational risk assessment

System, hazards, controls, residual risk and review criteria.

Product	Context
Code	CTX-PUB-14-EN
Document edition	Edition dated 29 July 2026
Effective / review	2026-07-29 / 2027-01-29
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 Calmaggione 5, 31100 Treviso (TV), Italia, VAT No. IT 05614380268 ("Niltech"), adopts this document in order to document system, context, hazards, exposed persons, controls, residual risk, acceptance criteria and suspension conditions.

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 assessment is continuous and records harm scenarios, exposed persons, measures, effectiveness, residual risk and decision. It does not assign an abstract immutable class to the product: legal qualification depends on intended purpose and concrete circumstances.

Personal and material scope

The objective scope includes Context, its public interfaces and processing strictly connected with the described functions. The Context website and service are made available through context.andreaaiagent.com and use Bluehost infrastructure. OpenAI provides AI processing services; MySQL, Redis, ClamAV, Tesseract, Poppler, ImageMagick and Exim/sendmail are technical components managed within the service environment and are not, for that reason alone, separate subprocessors. Legal-research functions, where enabled by the Customer and relevant to the request, may query public institutional sources including Cassazione/SentenzeWeb, Normattiva, AGCM and ANAC; an institutional source does not relieve the user from verifying currency, relevance and the applicable official text.

The relevant operations concern document upload and classification, text extraction and OCR, assisted analysis and synthesis, report drafting, review and research over enabled legal sources. Potential information categories are: authorised accounts, case files, documents, extracted text, OCR results, notes, legal sources, operational logs 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 Context 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 decompose the system into verifiable use cases and components. 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 identify harm from error, omission, bias, misuse, data and unavailability. 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 estimate likelihood and impact using stated criteria. 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 associate preventive, detective and corrective controls with each risk. 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 assess effectiveness with tests, samples, results and limitations. 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 accept, mitigate, avoid or transfer risk with owner and due date. The applicable file identifies the owner, scope, dependencies, acceptance criterion and evidence; absent those elements, the safeguard is not treated as demonstrated.

System and context

Context: document upload and classification, text extraction and OCR, assisted analysis and synthesis, report drafting, review and research over enabled legal sources.

The Context website and service are made available through context.andreaaiagent.com and use Bluehost infrastructure. OpenAI provides AI processing services; MySQL, Redis, ClamAV, Tesseract, Poppler, ImageMagick and Exim/sendmail are technical components managed within the service environment and are not, for that reason alone, separate subprocessors. Legal-research functions, where enabled by the Customer and relevant to the request, may query public institutional sources including Cassazione/SentenzeWeb, Normattiva, AGCM and ANAC; an institutional source does not relieve the user from verifying currency, relevance and the applicable official text.

Key risks

- inaccurate, incomplete or outdated outputs
- over-reliance and improper automation
- unnecessary personal or confidential data
- bias, loss of context or misinterpretation
- unavailability, supplier dependency or hostile use



Controls

Limited intended use, notices, human review, authorised access, source and document revision traceability where available, supplier management, testing and incident reporting reduce but do not eliminate risks.

Residual risk and review

Residual risk ranges from low to high depending on data and decision impact. Uses with legal, financial, insurance or rights effects require approval, enhanced control and, where necessary, suspension.

Review at least every six months and upon any change in model, provider, purpose, data category, incident or requirement.

Scope, audience and status of this document

This document is intended for customers, prospects, authorised users, advisers and control functions needing to understand the Context scope. Its specific objective is to document system, context, hazards, exposed persons, controls, residual risk, acceptance criteria and suspension conditions. 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 Context website and service are made available through context.andreaaiagent.com and use Bluehost infrastructure. OpenAI provides AI processing services; MySQL, Redis, ClamAV, Tesseract, Poppler, ImageMagick and Exim/sendmail are technical components managed within the service environment and are not, for that reason alone, separate subprocessors. Legal-research functions, where enabled by the Customer and relevant to the request, may query public institutional sources including Cassazione/SentenzeWeb, Normattiva, AGCM and ANAC; an institutional source does not relieve the user from verifying currency, relevance and the applicable official text.

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: The documented scope includes the website, application service, technical components and external sources used under the agreement.

- 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

Conditional classification conclusion

Document and drafting support for a professional is not, for that reason alone, the Annex III high-risk use concerning the administration of justice. Use by or on behalf of a judicial authority to research and interpret facts or law and apply the law to a concrete case may fall within that category; that purpose is outside the described use and requires prior classification, governance and any specific compliance measures.

The conclusion applies only to the described intended use, with auxiliary output and effective human review. It is not a permanent certification: substantial modification or a new purpose may change the role, risk category and duties.

Harm scenarios and affected persons

The assessment considers users, persons mentioned in files, customers, counterparties, professionals and third parties. Risk is not limited to technical malfunction: it includes discrimination, loss of confidentiality, professional error, economic harm, inability to challenge and use of a result out of context.

- non-existent citation, superseded source, OCR error or loss of legal context
- exposure of professional-secrecy material, judicial data or litigation strategy
- over-reliance on output, automation bias or failure to escalate uncertainty
- unavailability, supplier dependency, attack or manipulation of inputs and instructions

Method, residual risk and decision

For each scenario, the controlled register identifies cause, event, harm, affected person, likelihood and severity under a defined scale, preventive and detective controls, testing, owner and residual risk. A control receives credit only if applicable to scope and supported by evidence; a documentary statement alone does not reduce risk.

Residual risk is accepted, mitigated, transferred or leads to prohibition/suspension by a person with suitable authority. This document does not state a numerical rating or acceptability conclusion without the supporting evidence file.

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 Context 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 2026-07-29. 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 — Guidelines on Article 50 AI Act transparency obligations, July 2026
- Regulation (EU) 2016/679 (GDPR)

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.