



SECURITY & COMPLIANCE

Data protection impact assessment summary

Structured assessment of necessity, proportionality, risks and mitigations.

Product	Andrea AI
Code	AND-PUB-16-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 summarise description, necessity, proportionality, risks to people, measures, residual risk and the controlled DPIA decision.

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 summary reflects the method required by Article 35 GDPR and Guidelines WP248 rev.01. The full assessment remains a controlled accountability record; where high risk cannot be mitigated, processing may not commence without the determinations required by Article 36 GDPR.

Personal and material scope

The objective scope includes Andrea AI, its public interfaces and processing strictly connected with the described functions. The commercial website and document library are published on andreaaiagent.com and use Bluehost infrastructure, MySQL and server mail transport. The application is made available through the separate andreaai.net domain on Hetzner infrastructure; Pinecone, Cloudflare, OpenAI and Google Gemini are involved only within the functions and agreements applicable to them.

The relevant operations concern document and image intake and analysis, policy-reading support, estimates and report drafts, case-file organisation, and ESG indicators only where supported by verifiable data. Potential information categories are: contact and prospect data on the website; in the application, case data, documents, images, notes, technical metadata and AI-assisted outputs according to configuration and contract. 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 Andrea AI 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 map purposes, roles, subjects, data, sources, recipients and flows. 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 lawful bases, transparency, minimisation, quality and rights. 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 consider special data, vulnerability, scale, monitoring and new technologies. 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 assess access, exclusion, error, bias and loss-of-control risks. 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 link measures to evidence and assess effectiveness. 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 stop or consult where unmitigable high risk remains. The applicable file identifies the owner, scope, dependencies, acceptance criterion and evidence; absent those elements, the safeguard is not treated as demonstrated.

Scope and roles

The commercial website and document library are published on andreaaiagent.com and use Bluehost infrastructure, MySQL and server mail transport. The application is made available through the separate andreaai.net domain on Hetzner infrastructure; Pinecone, Cloudflare, OpenAI and Google Gemini are involved only within the functions and agreements applicable to them.

The customer is normally controller for operational data; Niltech processor. Niltech is controller for its own administrative and security data.

Data, purposes and bases

contact and prospect data on the website; in the application, case data, documents, images, notes, technical metadata and AI-assisted outputs according to configuration and contract

Purposes: document and image intake and analysis, policy-reading support, estimates and report drafts, case-file organisation, and ESG indicators only where supported by verifiable data.

Bases and necessity must be confirmed by the controller for the specific use; special-category data requires an additional condition.

Risks and measures

Risks: improper access, disclosure, excessive retention, wrong output, loss of control, transfer and supplier dependency. Measures: minimisation, access, logging, contracts, human review, incident handling, retention and supplier review.



Outcome and consultation

The full DPIA is in the controlled pack. Residual risk must be accepted by the competent owner; if it remains high without adequate mitigation, use does not proceed and authority consultation is considered.

Scope, audience and status of this document

This document is intended for customers, prospects, authorised users, advisers and control functions needing to understand the Andrea AI scope. Its specific objective is to summarise description, necessity, proportionality, risks to people, measures, residual risk and the controlled DPIA decision. 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 commercial website and document library are published on andreaaiagent.com and use Bluehost infrastructure, MySQL and server mail transport. The application is made available through the separate andreaai.net domain on Hetzner infrastructure; Pinecone, Cloudflare, OpenAI and Google Gemini are involved only within the functions and agreements applicable to them.

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 commercial website, the public library and, where expressly stated, processing connected with the application.

- 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



Nature of the summary and ownership of the decision

This summary describes the method and areas requiring assessment; it does not prove that a complete DPIA has been concluded for every Customer or configuration. The controller is responsible for determining whether processing is likely to result in high risk and, if so, completing the assessment before processing. Niltech provides information reasonably available to it as processor.

A DPIA must describe operations, purposes and any legitimate interest; assess necessity and proportionality; consider risks to rights and freedoms and their sources; define measures, safeguards and demonstration mechanisms; seek data-subject views where appropriate; record the DPO's advice if one is appointed and the controller's decision.

Risk factors to examine

Insurance files may contain health data, images of individuals, vehicle-registration numbers, contact details, financial information and, in fraud or litigation matters, criminal-offence data. Such data may not be submitted merely because it is convenient: the Customer must document an Article 6 GDPR basis and, where relevant, an Article 9 or 10 condition, minimise the data and restrict access to authorised persons.

Volume and duration, monitoring, vulnerable individuals, source combination, transfers, supplier access, ability to challenge, AI error, professional reliance, security, deletion and material consequences are also considered. Necessity and proportionality are assessed against less intrusive alternatives.

Where high risk remains after measures and the controller cannot reduce it, processing does not begin before consulting the authority under Article 36 GDPR. Review is mandatory when risk, purpose, model, supplier, flow or law changes.

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 Andrea AI 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) 2016/679 (GDPR)
- Guidelines WP248 rev.01 on data protection impact assessment
- Italian Data Protection Authority — Data protection impact assessment

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.