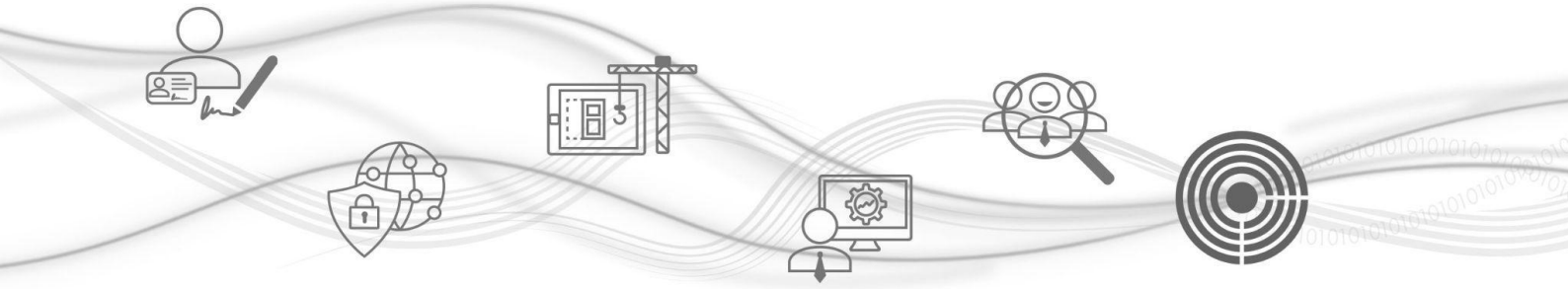
Namirial Onboarding Operating Manual

Practice Statement for Remote Identity verification service



Category	**Operating Manual**	Document Code	**NAM-NOB-MO**	**Namirial S.p.A.**
Written by	**Team Compliance**	Classification	**Public document**	**The Legal Representative**
Verified by	**Libero Rignanese**	Version	**1.3**	**Massimiliano Pellegrini**
Approved by	**Massimiliano Pellegrini**	Date of issue	**08/06/2026**	--

Signed by: PELLEGRINI MASSIMILIANO
Issued by: Namirial CA Firma Qualificata
Signing time: 24-07-2026 08:57:31
IP address: 185.5.246.18

Namirial S.p.A.
Via Caduti sul Lavoro n. 4, 60019 Senigallia (An) - Italy | Tel. +39 071 63494 | www.namirial.com | amm.namirial@sicurezzapostale.it | P.IVA IT02046570426 C.F. and registration at Ancona Companies Reg. N. 02046570426 | REA N. AN – 157295 Addressee code T04ZHR3 | Share capital € 8,256,361.60 fully paidaid-up Company subject to the management and coordination of Ink (BC) Holdco Spa – Tax Code 14254460968

INDEX

Change history

Version	Date	Motivation	Edit
1.3	08.06.2026	Update	Revision of paras. 9 and 12; Introduction of a framework based on two operating models (QTSP Partner / Non-QTSP Partner).
1.2	29.10.2025	Update	Addition of new onboarding flow (§ 4.3.1); Addition of active liveness detection (§ 4.3.1)
1.1	15.09.2025	First issue of the document	Consolidated version with technical information
1.0	28.08.2025	First draft	

Technical and regulatory references

In providing the service, Namirial S.p.A. complies with the applicable European and national rules and regulations. The main regulatory references are shown in the following table.

LEGISLATION	DESCRIPTION
eIDAS 910/2014	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
eIDAS 1183/2024	Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards the establishment of the European Digital Identity Framework
ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI EN 319 411-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI EN 319 411-2	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
ETSI EN 119 461	Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
GDPR (EU) 2016/679	REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)
ICAO Doc 9303 pt.3	Machine Readable Travel DocumentsPart 3: Specifications Common to all MRTDs
ICAO Doc 9303 pt.4	Machine Readable Travel Documents: Part 4: Specifications for Machine Readable Passports (MRPs) and other TD3 Size MRTDs
ICAO Doc 9303 pt.10	Machine Readable Travel Documents: Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)

Figure 1: Technical and regulatory references

Definitions and acronyms

The following are the meanings of the specific acronyms and terms, except for those in common use.

Term or Acronym	Meaning
AgID [Agenzia per l'Italia Digitle]	Italian government body responsible for promoting digital innovation and defining technical rules for public administration information systems.
APCER [Attack Presentation Classification Error Rate]	Error rate with which the system mistakenly accepts an attack presentation as if it were genuine.
Applicant	A natural person who applies to the IPSP for identity verification and the issuance of Qualified Certificates, whose identity must be proven.
Attribute	Structured information associated with an individual, object or service, used to describe its characteristics, properties, roles or operating conditions within the trust service.
Audit trail	A document containing the set of historical records documenting all identity verification operations.
Authentication	Process for verifying the identity or authenticity of an individual, device or process, as a prerequisite for access to trust systems, data or services.
AVA [Advanced vulnerability assessment]	Vulnerability assessment that measures the resilience of a product or system to potential attacks.
BAC [Basic Access Control]	Access control mechanism defined by ICAO Doc 9303 specifications, used in electronic travel documents to limit access to data stored in the contactless chip only to subjects in possession of the information present in the MRZ (Machine Readable Zone) of the document.
BPCER [Bona Fide Presentation Classification Error Rate]	Error rate with which the system mistakenly rejects a genuine (non-attack) presentation.
CA [Certification Authority]	A trusted entity responsible for issuing, managing, suspending, revoking, and renewing digital certificates as part of a public key infrastructure (PKI), as well as verifying the association between the entity's identity and its public key.

Term or Acronym	Meaning
CIE [Electronic Identity Card]	Electronic identity document issued by the Italian government, compliant with European standards and ICAO Doc 9303 specifications, equipped with a contactless microprocessor containing identification data, biometrics and electronic certificates that can be used for the physical and digital identification of the holder.
Digital identity document	Identity document issued in electronic format, equipped with logical and/or cryptographic security elements (e.g. chips, digital certificates or verifiable credentials), which allows the certain identification of the holder both in physical and digital contexts, also for the purpose of authentication to online services.
Electronic document	Document drawn up and stored in digital format, which can be consulted and managed using computer systems.
Electronic identification	Process of using personally identifiable data in electronic form to prove the identity of a natural or legal person in a digital system, pursuant to Regulation (EU) eIDAS.
eID [Electronic Identity]	A set of electronic data and credentials representing the identity of an entity in the context of trust services and electronic identification systems, within the meaning of Regulation (EU) eIDAS.
eIDAS	Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market, as amended by Directive (EU) 2022/2555 and Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards the establishment of the European Digital Identity Framework, provides a regulatory framework for the electronic identification of natural and legal persons and for services trustees.
eMRTD [Electronic Machine-Readable Travel Document]	Electronic travel document compliant with ICAO Doc 9303 specifications, equipped with a contactless chip that stores the holder's personal, biometric and security data, used for identification and automated identity verification at border crossing points.
EUDI Wallet	Secure digital wallet that allows European citizens, residents and businesses to store and manage their identity credentials and official documents (e.g. driving licences, diplomas) in electronic form.
Face matching	Biometric process of comparing two images of the face in order to verify that they belong to the same person.

Term or Acronym	Meaning
FAR [False Acceptance Rate]	Performance indicator of biometric systems that measures the probability that the system will mistakenly accept an unauthorized person or one who does not correspond to the declared identity.
FRR [False Rejection Rate]	Performance indicator for biometric systems that measures the likelihood that the system will mistakenly reject a legitimate person by not recognising the correct identity.
GDPR [General Data Protection Regulation - EU Regulation 2016/679]	Fundamental legislation of the European Union that regulates the protection and processing of personal data. Its aim is to give citizens back control over their data and standardise privacy across the EU.
IAD [Injection Attack Detection]	Set of logical and/or hardware controls and countermeasures intended to identify attempts to manipulate the data flow in electronic or biometric identification systems, in which synthetic or non-synthetic inputs from the authentic sensor are injected to evade authentication or acquisition mechanisms.
Identity document	A document issued by a public or recognised authority, in paper or electronic form, which allows the unique identification of the holder and can also be used for authentication in physical and digital contexts.
Identity proofing	Process by which the declared identity of a subject is verified through the acquisition, validation and correlation of identification, documentary and biometric evidence, in order to establish an adequate level of identity reliability.
IPSP [Identity Proofing Service Provider]	Person or entity responsible for carrying out the process of verifying the identity of a natural or legal person, through the use of documentary, biometric or electronic procedures and checks, in order to establish with a predefined level of reliability the correspondence between the declared identity and the real identity.
Liveness detection	Process of verifying that the person being identified is a real natural person, present and alive at the time of the identification session, by thwarting attempts at impersonation through photographs, pre-recorded videos, masks, deepfakes or other artifacts.
LoA [Level of Assurance]	The level of trust attributed to the electronic identification process and the means used to verify the identity of an individual, which describes the degree of certainty that a given identity is correctly established and managed.

Term or Acronym	Meaning
LoIP [Level of Identity Proofing]	Level of rigor applied in the process of verifying the identity of an individual, which describes the intensity and depth of the checks carried out to establish the correspondence between the declared identity and the real one, depending on the risk and the context of use.
MRZ [Machine Readable Zone]	A standardised portion of an identity or travel document, in accordance with ICAO DOC 9303 specifications, consisting of one or more lines of machine-readable optical characters, containing essential data of the holder encoded according to a predefined format for reading by automatic systems.
Namirial PID	Service or component offered by Namirial for the issuance, management and validation of PID (Person Identification Data) within digital identity solutions and wallets compliant with Regulation (EU) eIDAS 2, used to certify in electronic form the identification attributes of a natural person in a verifiable and interoperable way.
NFC [Near Field Communication]	Short-range wireless communication technology that allows the exchange of data between compatible devices placed at a very close distance (typically a few centimeters), based on electromagnetic coupling and used for authentication, identification and contactless payment.
OCR [Optical Character Recognition]	Optical character recognition: technology that allows the automatic conversion of text present in images, scanned documents or visual supports into digital textual data, making them processable by computer systems.
OID [Object Identifier]	A globally unique and hierarchical identifier used to unambiguously name objects, attributes, algorithms, or policies within information and cryptographic systems, particularly in PKI and x.509 standards.
Onboarding	Process by which an individual is registered and enabled to use a service, following the activities of identification, identity verification, acquisition of the necessary information and acceptance of the applicable conditions.
PAD [Presentation Attack Detection]	Set of techniques and controls used in biometric systems to detect and prevent presentation attacks, i.e. attempts to deception the biometric sensor through the use of artifacts (e.g., masks, photographs, artificial fingerprints, replays, or deepfakes) in order to impersonate a legitimate person.

Term or Acronym	Meaning
PEACE [Password Authenticated Connection Establishment]	Advanced cryptographic protocol defined in the ICAO DOC 9303 specification to establish a secure communication channel between a reader and the chip of an electronic travel document, based on authentication via password or equivalent information and designed to replace or supplement the BAC, offering a higher level of security against eavesdropping attacks and unauthorized access.
Physical ID	Identity document issued in paper or plastic form by a competent authority, which allows the visual and, if applicable, automatic identification of the holder by means of physical and/or machine-readable security elements (e.g. MRZ, barcode, contactless chip).
PID [Person Identification Data]	Structured set of data representing the identity of a natural person, including identifying attributes and associated information used for identification and authentication in digital systems, in particular in the context of eIDAS 2 and digital identity wallets.
PRADO [Public Register of Authentic identity and travel Documents Online]	Official database managed by the Council of the European Union that provides information on the security features and formats of authentic travel and identity documents issued by EU Member States, as well as by certain third countries. It is primarily intended for use by public authorities, border control officers, and others involved in identity verification.
QTSP [Qualified Trust Service Provider]	Qualified trust service provider that provides one or more qualified trust services and has been recognised as such by the competent supervisory body pursuant to Regulation (EU) No 910/2014 (eIDAS) and its implementing provisions.
Qualified Certificate	Electronic certificate compliant with the requirements of Regulation (EU) No. 910/2014 (eIDAS), issued by a qualified trust service provider (QTSP), which certifies the identity of the holder and associates this identity with the verification data of the electronic signature, allowing the creation of a qualified electronic signature with legal value equivalent to the handwritten signature.
Qualified timestamp	Electronic evidence generated by a timestamping authority that reliably binds a data hash to a time reference, ensuring proof of the existence, integrity, and non-alteration of the data over time, according to the requirements of Regulation (EU) eIDAS and ETSI standards for trust services.

Term or Acronym	Meaning
Relying Party	An entity that receives and uses identity claims, digital certificates, or other trust services issued by an identity provider or certificate authority, and is responsible for validating the trust of the identity provider or certificate authority for authentication or authorization.
SPID [Public Digital Identity System]	Italian national digital identity system that allows citizens and businesses to access the online services of the public administration and participating private entities, through credentials issued by accredited identity providers and based on different levels of security and authentication.
Trust Service [Trust Service]	eIDAS (EU) service that supports the creation, verification and validation of reliable electronic data, including certificates, electronic signatures and seals, timestamps and certified electronic delivery services, provided by a qualified or non-qualified provider.
VIZ [Visual Inspection Zone]	Visual area of an identity or travel document, intended for the manual reading and verification of printed information, including the holder's personal details and security elements visible to the naked eye or with magnifying tools.
WSCD [Secure Cryptographic Device Wallet]	Hardware element with security and tamper resistance characteristics, used in digital identity systems to perform cryptographic operations in an isolated and trusted environment, in particular in the context of eIDAS 2 compliant digital identity wallets.
Web Interface	Interface accessible via browser for interaction with a computer system.

Figure 2: Definitions and acronyms

Brief description of Namirial S.p.A.

Namirial S.p.A. is an Italian multinational Information Technology company with registered office in Senigallia (Ancona), active in the Digital Transaction Management (DTM) sector. Founded in 2000, the company develops solutions and technologies for digital identity verification, electronic signature, electronic invoicing and the secure management of digital document flows. With over 1,000 employees and offices distributed throughout the country and in various European and non-European countries, Namirial today serves a clientele ranging from professionals and SMEs to large enterprise organizations, public administrations and operators of regulated markets, to whom it provides high value-added digital services integrated into their respective business processes.

Namirial is a Qualified Trust Service Provider (QTSP) pursuant to the eIDAS Regulation (EU No. 910/2014) and is registered in the public list of qualified trust service providers held by AgID – Agency for Digital Italy. The portfolio of trust services has been consolidated over time through successive qualifications: from the management of Certified Electronic Mail (since 2007) and the digital storage service in accordance with the law (since 2014), to qualified electronic signature (since 2010), up to accreditation as an Identity Provider within the SPID Public Digital Identity System (since 2017). These are now flanked by advanced digital onboarding and remote identity verification solutions, delivered in API-first mode for the benefit of customers who integrate Namirial services into their operational flows.

Namirial S.p.A. is:

Qualified Trust Service Provider eIDAS

Namirial is QTSP according to the eIDAS definition for services:

- Issuance of the qualified certificate for electronic signature;
- Issuance of the qualified certificate for the electronic seal;
- Issuance of the qualified timestamp;
- Preservation of qualified signatures and qualified seals

Namirial is listed in the EU Trust Services Dashboard and is accredited by the Italian government as a trust service provider.

Trust service providers active in Italy

Certificate 910/2014 eIDAS – Qualified Trust Service Providers

Electronic Registered Delivery – PEC Manager

accredited by AgID and authorized to manage Certified Electronic Mail (PEC) mailboxes and domains, it has been providing the Postal Security service since 2007.

List of PEC operators

The service is SaaS qualified QC1 level by ACN and included in the Digital Infrastructure and Cloud Services Catalog

Digital Infrastructure and Cloud Services Catalogue – PEC

Electronic Identification – Identity Provider SPID

Namirial provides SPID digital identification trust services and is accredited by the Italian government according to the European eIDAS standards pursuant to:

- Prime Ministerial Decree 24/10/2014;
- Commission Implementing Regulation EU 2015/1502;
- Regulation (EU) 910/2014 eIDAS, art. 24 for the provision of trust services of Digital Identification.

Accredited identity providers

ETSI EN 319 401 certification

Long Term Archiving Provider -Soggetto Conservatore
in accordance with:

- Technical Rules pursuant to art. 71 of the Digital Administration Code;
- Regulation (EU) 910/2014 eIDAS, art. 24 for the provision of fiduciary services of Conservation in accordance with the law.

Namirial has been providing the Long-Term Archiving service since 2014, it is qualified by AgID and the Cybersecurity Agency.
The service is SaaS qualified QC2 level by ACN and included in the Digital Infrastructure and Cloud Services Catalog.
Qualified Conservators
Digital Infrastructure and Cloud Services Catalog – NamirialArchive

UNI EN ISO 9001:2015 certified. Namirial has obtained the **Quality Management System** certificate issued by Bureau Veritas Italia S.p.A.

ISO/IEC 27001:2022 certified. Namirial has obtained the **Information Security Management System certificate integrated with the controls provided for by the ISO/IEC 27017:2015 and ISO/IEC 27018:2019 guidelines** issued by Bureau Veritas Italia S.p.A.

ISO 37001:2016 certified
Namirial has obtained the **Anti-bribery management systems** certificate issued by Bureau Veritas Italia S.p.A.

UNI PdR 125:2022 certified
Namirial has obtained the **Gender Equality Management System certificate** issued by Bureau Veritas Italia S.p.A.

Certified by Adobe. Since June 2013, Namirial has been a member of the AATL (Adobe Approved Trust List).

1 INTRODUCTION

1.1 Purpose and scope

This document is an Operating Manual issued by Namirial S.p.A. and describes the operating rules and procedures adopted by Namirial for the provision of the **Onboarding service.**

This document outlines the rules and standards adopted by the **Identity Proofing Service Provider** Namirial S.p.A. for the provision of identity verification services for individuals through an **unattended remote video-identification system**.

The *Partner Addendum*, signed between Namirial and each Partner prior to the activation of this service, is an integral part of this Operating Manual. It defines all the Partner's specific provisions regarding data protection, obligations towards applicants, allocation of liability, insurance coverage and contractual conditions.

Two versions are available:

- the Namirial QTSP Partner Addendum, pre-filled with Namirial data, applicable if Namirial acts as both an IPSP and a QTSP;
- the Partner Template Addendum, to be completed and signed by any other Partner. In the event of a conflict between this Operating Manual and a signed Partner Addendum, the Partner Addendum shall prevail for the matters it governs.

1.2 Document name and identifier

This document, called "*Namirial Onboarding Operating Manual Practice statement for the remote identity verification service*", with document code **NAM-NOB-MO** is identified by the version level and the date of release on all pages. The preamble to the document also includes a paragraph with the history of the changes made.

Namirial carries out, at least once a year, a compliance audit of the Onboarding service and, where necessary, updates this document according to the evolution of legislation and technological standards.

This document and any additional documents issued for specific matters or cases, as *an addendum* to this Operating Manual, are published by Namirial and can be consulted electronically at the following address:

https://www.namirial.com/it/documentation/

The document is published in signed PDF format to guarantee its origin and integrity.

1.3 Participants and responsibilities

1.3.1 Subjects involved

The subjects mentioned in this document are:

a) **IPSP (Identity Proofing Service Provider):** Identity verification Service Provider;
b) **Applicant:** the natural person who submits the verification request and performs the identification;
c) **Relying Party**, the natural or legal person who relies on the identity verification service or a trust service;
d) **Back-office** operators.

1.3.1.1 Identity Proofing Service Provider

An Identity Proofing Service Provider (IPSP) is a qualified or accredited entity that provides identification services.

Namirial S.p.A. is an accredited Trust Service Provider recognized by a supervisory body (such as AgID in Italy or at EU level), which issues qualified digital services such as qualified electronic signatures and electronic seals.

In this case, the QTSP also acts as an IPSP, directly performing identity proofing verifications in accordance with ETSI EN 319 461 standards.

The full details of the organisation acting as an IPSP are as follows:

Company name	Namirial S.p.A.
Registered office	VIA CADUTI SUL LAVORO, 4 60019 – SENIGALLIA (AN) +39 071.63494
VAT number	IT02046570426
Service Website	https://www.namirial.com/it/onboarding/
Website	http://www.namirial.com

Figure 3: Identity Proofing Service Provider identifiers

1.3.1.2 Applicant

A natural person whose identity undergoes the onboarding process for the purpose of issuing or using a trust service.

1.3.1.3 Relying Party

An individual who relies on the outcome of the onboarding process or associated trust services, assuming verified identity information is valid.

1.3.1.4 Back-Office Operator

A back-office identity verification operator is a person who is properly trained to verify the identity of an Applicant, using specific procedures and technologies.

Back-office operators must:

- be authorized to carry out identity verification operations by a certified IPSP or TSP;
- operate in compliance with the operating procedures and safety requirements defined by the IPSP or TSP;
- guarantee the confidentiality, integrity and protection of personal data and information processed during the performance of onbaording activities, in compliance with Regulation (EU) 2016/679 (GDPR) and the applicable legislation on the protection of personal data;
- verify and process identification evidence exclusively within the scope of the assigned authorizations;
- promptly report anomalies, security incidents, suspicions of fraud or non-conformities detected in the identification process;
- use secure platforms for real-time or deferred video identification;
- maintain adequate levels of training, competence and updating in relation to identity verification and fraud detection procedures;

2 ADMINISTRATION OF THE OPERATING MANUAL

2.1 Publishing and archiving

The responsibility for this document lies with the role of 'Service Manager', who is responsible for verifying, publishing and updating.
Communications relating to this document may be sent to the attention of the aforementioned manager at the following addresses:

E-mail: infotsp@namirial.com

Since a specific Object Identifier (OID) is not required for the service covered by this document, the OID that identifies Namirial S.p.A. is iso(1) identified-organisation(3) dod(6) internet(1) private(4) enterprise(1): 36023:

OID: 1.3.6.1.4.1.36203

The Namirial repository is available at:

https://www.namirial.com/en/documentation/

This document is publicly available and read-only. Namirial manages the accessibility of the repository autonomously and continuously (24x7x365) and is directly responsible for it.

This document is published whenever it is updated.

3 ONBOARDING OPERATIONS

The main purpose of Remote Onboarding is to verify the identity of the person undergoing the identification process to ascertain that he or she is who is claimed to be and to enable them to use the requested service in compliance with applicable regulatory, contractual and security requirements. The solutions aim to validate the identity of natural persons.

The NOB solution is composed of technological modules that, individually or in combination, allow a secure digital onboarding process compliant with the requirements of identity proofing, security, reliability, traceability and evidence management provided by the ETSI TS 119 461 V2.1.1 standard and the applicable eIDAS regulatory framework. In particular, the solutions ensure a secure and reliable method for the identification of natural persons in accordance with the requirements of ETSI 119 461 and the Implementing Act of Article 24 of the eIDAS Regulation.

With the controls described in the following paragraphs, you will be able to implement the solutions and processes outlined in paragraph 4.

3.1 Data collection

The procedure requires the Applicant to use a device connected to the Internet (tablet, smartphone or PC) equipped with a working webcam. An automated process guides the Applicant through an end-to-end workflow for an unattended remote identification experience.

Each session is initiated via a secure communication channel, ensuring confidentiality and integrity.

Before starting the identification procedure, the Applicant is informed in advance, in a clear and understandable manner, about the purpose of the onboarding process, the methods of processing personal data, the terms and conditions applicable to the service as well as the obligations arising from the use of the same. The Applicant must also read the privacy policy and explicitly accept the terms and conditions of the service, giving the required consents in accordance with the requirements of the onboarding process.

Figure 4: Onboarding Initiation Flow

Subsequently, the Applicant is asked to properly place the ID document within a special box to allow the application to capture a short video recording of the document, capturing both the front and the back. The application will refrain from scanning the image if the document is not correctly framed or the image is not fully legible.

Following the acquisition of the document, the procedure uses an advanced OCR system to:

- extract relevant data from the identity document, including the Applicant's first and last name, date of birth, document number and photograph;
- extract the data present in the MRZ (Machine Readable Zone).

Several checks are performed to determine the authenticity and validity of the identity document, including:

- checks on optically variable elements (OVDs);
- machine-readable zone (MRZ) checksum checksums;
- cross-checks between the data present in the optical reading zone (MRZ) and those present in the visual inspection zone (VIZ).

The acquisition of the identity document takes place exclusively through a web interface, external document uploading is not allowed.

The Applicant will also be asked to make a short aimed video recording at verifying the liveness (liveness detection). The viability check can be carried out by means of active or passive mechanisms, depending on the type of identification process adopted.

In the case of identification using pre-existing eID means, no additional actions will be required outside of selecting the eID provider and authenticating with the method supported by the eID; the system will retrieve the information on personal attributes and associate it with those relating to the requested service (§ 3.3).

In order to ensure the protection and management of personal data in full compliance with Regulation (EU) 2016/679 (GDPR), each Applicant is provided with the privacy policy in advance.

3.1.1 Accepted identification documents

The Applicant may identify himself or herself by means **of a valid physical or digital identity document**, in its original form.

By way of example, a list of accepted identity documents is provided, only if they are valid, bearing the Applicant's photograph and issued by a State administration:

- ID card,
- Passport,

The documents that can be submitted can be found in the PRADO database, at the following link https://www.consilium.europa.eu/prado/en/prado-start-page.html.

An identity document includes two main categories of information:

- The Visual Inspection Zone (VIZ), which reports the personal data of the document holder. This section includes:
  - Face Image: a photograph that represents the identity of the person.
  - OCR Data Fields: Coded textual data such as first names, surnames, dates, identification numbers, document serial numbers, and similar information.
  - Physical Security Features: Built-in physical protections including optically variable inks (OVIs), microprinting, kinegrams, and other anti-counterfeiting features.
- The Optical Reading Zone (MRZ), is the area of the ID document where machine-readable information appears. It is generally composed of two lines (passport) or three lines (identity card).

In case of an invalid document, the process will fail.

3.1.2 Types of data collected

This section summarises the types of data collected during the onboarding and registration processes. The data is classified as **mandatory** when required for regulatory compliance or for fundamental functionalities of the service (such as first name, last name and personal identification number), and **optional** (or supplemental) when collected for additional verification purposes.

The set of mandatory data extracted and collected includes:

- Name
- Surname
- Document number
- Country of issue
- Valid from (date)
- Valid until (date) – if available in the document

- Date of birth
- Place of birth
- Nationality
- Place of issue
- Gender
- Tax ID or personal identification number

The acquisition of identification data takes place directly from the source of identity used in the process (eID or identity document), in order to ensure the accuracy of the information collected and reduce the risk of errors resulting from manual transcription. In the case of documents equipped with a machine-readable zone (MRZ), data extraction is carried out primarily by acquiring the information contained in the MRZ itself.

If the identification process is initiated by a native application that includes the Namirial Onboarding SDK and the Applicant provides digital identification documents (compliant with ICAO 9303 Part 10 [9] with MRZ or similar characteristics), the NFC ID may be used.

3.2 Data validation

The data validation process involves the documentary verification of the evidence presented by the Applicant, specifically the verification of the identity document

The validation of the data from the identity document is a critical part of the overall verification process. In cases of attempted fraud, two common scenarios typically occur:

- Fake identity documents, entirely counterfeit;
- Forged identity documents, where authentic documents have been altered or tampered with.

During the validation process, all personal data and documentary information provided by the Applicant are subjected to structured validation to ensure accuracy, authenticity and reliability.
The system automatically performs logical consistency checks such as:

- verification of the integrity of the document;
- verifies the consistency of the information captured on all relevant fields, including name, date of birth and document number;
- specific validation on machine-readable elements, such as MRZ, including checksum verification.

In addition, the system verifies the authenticity of the identity document by detecting possible signs of tampering, verifying the consistency between MRZ and VIZ and analysing specific security elements (such as, for example, holograms, official fonts, border

formatting), including checks against replay attacks and attempts to forge by reproduction or printing of the document. The data extracted from the MRZ are then validated and compared with the information in the visible part of the document.

The system also makes it possible to detect cases in which the same identity document is presented several times, even if some personal data (such as, by way of example, name, surname, date of birth and place of birth) are modified or altered compared to previous presentations, through mechanisms of comparison and correlation of the evidence acquired.

Given that only official or nationally approved national registries should be accepted as trusted registries, and that availability varies from country to country, Namirial does not implement registries for attribute collection or validation. In addition, in the main jurisdictions in which Namirial operates, including Italy, France, Spain, Germany and Romania, there are currently no official or nationally approved databases available for the automated or real-time verification of identity attributes under conditions compatible with trust services operations. Accordingly, the identification of the Applicant is based on direct verification of documents and authoritative evidence provided by applicants or supervised entities.

The validation process can, depending on the use cases, be delegated and conducted by Namirial operators. In this case, the procedures established for the verification of identity documents are detailed in dedicated internal procedures and documentation, specifically adapted according to the country of issue of the document.

The process is considered completed with a positive outcome only after the validation of all the required data. Any inconsistencies, anomalies or unverifiable data will result in the rejection of the process or the activation of an escalation for further checks and investigations.

3.3 Identification using *eID means*

Identification via eID means occurs when the Applicant is identified through a pre-existing digital identity system.

This method requires that the Applicant is, therefore, in possession of a **pre-existing national electronic identification means**:

Specifically, Namirial provides that identification can also be performed by tools that guarantee the same level of reliability (high level of assurance) notified by other Member States and published by the European Commission in the Official Journal, in accordance with Article 9 of Regulation (EU) No. 910/2014 (eIDAS) and subsequent amendments,

which can be consulted at the following link: Overview of pre-notified and notified eID schemes

The integration allows applicants to access online services through credentials they already have; federated identities obtained under the various national digital identity programs and in compliance with the eIDAS Regulation.

The Applicant authenticates by entering the credentials, allowing the acquisition of certified data and accelerating the onboarding process. The system retrieves personal information and associates it with information related to the subscription service requested.

3.4 Binding to the Applicant

Binding to the Applicant is done through biometric technology and/or manual verification.

The procedures outlined below ensure consistency and repeatability, helping to avoid errors, fraud, or discrepancies in identity verification, ensuring a high level of security and reliability. Considering that identity theft is carried out with increasingly sophisticated techniques, the technologies implemented are advanced.

3.4.1 Biometric controls

The system implements biometric checks aimed to verify the identity of the subject during the remote identity proofing process, in accordance with the requirements of ETSI TS 119 461 v. 2.1.1 and the applicable biometric standards.
Biometric checking is the step in the process of remote unattended identity verification in which an individual's biometric data, such as facial features, is collected, analysed, and compared with data previously recorded or contained in a government identity document.

3.4.1.1 Biometric matching checks (*face matching*)

In a remote context, this check is typically performed using digital tools (such as a video camera) and **biometric match verification algorithms** that automatically analyse the user's physiological or behavioural characteristics from the biometric sample acquired during the session and the reference image associated with the declared identity.

The *face matching algorithm* is implemented 1:1 and ISO/IEC 19795 certified with the following performances:

- False Match Rate less than 0.1% on thousands of comparisons;
- False Non-match Rate of 0% on thousands of successful comparisons.

The biometric data extracted from the image undergoes multiple automated validations to confirm that the subject matches the photograph captured.

3.4.1.2 *Liveness* checks

Liveness detection is a security technique used in biometric verification to determine that captured biometric data, such as face, comes from a real, physically present person at the time the data is captured, rather than from a forged source.

Liveness detection can be implemented through:

- **Active liveness detection:** by the execution of certain actions (challenges) by the Applicant side:
    - The system verifies the Applicant's response in real time: in the event of a successful execution of the challenge, the system concludes that the subject is present, real and actively involved in the identification process, reasonably excluding the presence of spoofing attempts.
- **Passive liveness detection method**, which involves the analysis of vital presence indicators such as skin texture, eye movement or depth information, without requiring any user interaction:
    - The Applicant is asked to make a short video recording; a frame of the face is captured at a resolution suitable for automated analysis. If all quality parameters (such as lighting, positioning and resolution) meet the required standards, the system automatically acquires static images of the Requestor from the video stream. The biometric data extracted from the image undergoes multiple automated validations to confirm that the subject matches the photograph captured.

This phase involves the systematic application of anti-spoofing techniques, ensuring that the biometric data come from a living subject and not from a fraudulent source, responding to the need to verify the real presence and actual existence of the Applicant.

The technology of these detection components is implemented with **PAD (Presentation Attack Detection)** and **IAD (Injection Attack Detection)** and is certified 30107-3 Level 1&2 for PAD and CEN/TS 18099 high for IAD.
For the PAD, the APCER (Error Rate in Attack Classification) and the BPCER (Error Rate in the Classification of Authentic Presentations) are defined at 0% and up to 15%, respectively.

The components analyse multiple features within the image to identify artifacts and inconsistencies and detect spoofing attempts, such as:

- **Video Replay attack** — occurs when a malicious actor records a video in physical presence and attempts to reproduce it, via an external display, by placing it in front of the webcam used for the identification of an Applicant;
- **Printed Photo attack** — occurs when a malicious actor records a video or takes photographs and then prints one or more frames on paper to present them, via external display, in front of the webcam used for the identification of an Applicant;
- **3D Mask attack** — occurs when a malicious actor physically presents himself in front of the webcam used for the identification of the Applicant, using a physical artifact (such as, for example, a silicone or plastic mask) built to imitate the facial features of an individual;
- **Video Injection** – occurs when a malicious actor, through the use of specific software, pre-records a video of another individual who completes the entire identification process to inject it in real time into the onboarding flow, simulating a live session;
- **Deepfake Video Injection** — occurs when a malicious actor uses a synthetic or manipulated video via generative artificial intelligence techniques, which is fed into the video capture channel in order to simulate the presence of a legitimate subject during the biometric verification process., simulating a live session.

3.4.2 Manual verification

When manual verification occurs as part of the identity data validation process, the process is carried out, in the back-office, by an **expert human operator**, through real-time monitoring of onboarding sessions and with an updated view of all the checks performed and the actions to be taken.

This solution employs a team of anti-fraud experts, ensuring expertise and rapid response to emerging threats. These resources operate 24/7.

The controls consist of the following phases:

- the Applicant is asked to present a valid photo ID issued by a government authority. The operator examines the document in real time via video stream or high-resolution images, verifying:
  - Authenticity and integrity of the document (security elements, layouts, holograms, etc.)
  - Consistency of document data (name, date of birth, expiration date);
  - Readability and clarity of the MRZ area, where applicable.
- Examination of the results of the automated liveness detection system;
- Reviewing of the results of automated face matching by visual comparison between:
  - The Applicant's real-time face (captured via video or image);
  - The photograph on the identity document.

Whenever the operator finds uncertainties regarding the checks performed, he/she will suspend or refuse identification and/or escalate the file to a supervisor for further clarification.
The operator is responsible of documented decisions regarding the outcome of the identity verification. The session, including evidence (videos, screenshots, metadata), is recorded and stored securely in accordance with applicable regulatory requirements (e.g. GDPR, eIDAS).

3.5 Proof of evidence

At the end of the remote identification process, the system generates and stores the evidence associated with the identity proofing session, including the results of documentary, biometric and anti-fraud checks, time references and the elements necessary to ensure traceability, integrity and auditability of the process.

Documents and evidence are digitally stored in a secure storage system, ensuring the authenticity, integrity, availability and recoverability of archived documents for the period required by local regulations.

An **audit trail** is maintained, it documents the steps of the entire identification process, recording in chronological order each relevant status and event, in order to ensure full traceability and accountability proof of identity verification operations.
Metadata are included for all key steps in the process, such as document capture, data extraction, biometric analysis, physical presence detection, system-generated confidence scores, manual intervention (where applicable), and the final outcome of the verification. Each audit trail is stored securely and protected from tampering, through the affixing of a qualified electronic seal (eSeal), and is available for internal reviews or external audit activities, in line with applicable legal and regulatory requirements.

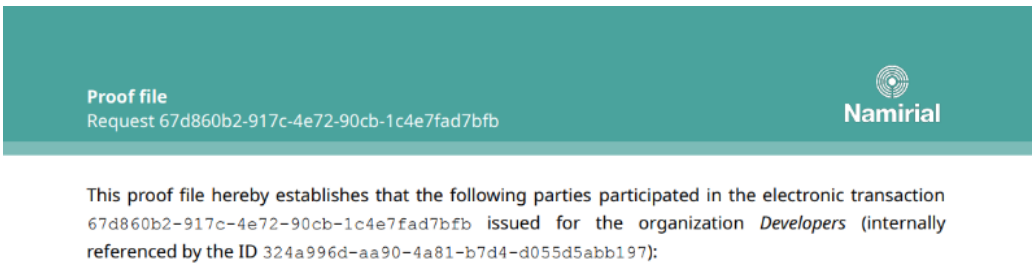


Figure 5: Top of the Audit Trail (test file)

By way of example, the audit trail includes the following elements:

- Date and time the request was created;
- Date and time of access of the Applicant to the NOB process;
- Browser and IP of the Applicant;
- Date and time of acceptance of the terms and conditions;

- Date and time of each document submission status;
- Details of the identity document submitted by the Applicant;
- Validation details.

The data and evidence are stored for a defined period in accordance with the applicable regulations, in order to ensure that they can be retrieved in the same period by authorized personnel.

4 NAMIRIAL ONBOARDING SOLUTIONS

The NOB suite is structured in a flexible and modular way; the combination of technology modules make possible to create a secure, compliant, and scalable remote onboarding process.

4.1 Identification with *eID LoA sub and ID Self Fast*

This identification flow combines LoA substantial eID authentication with document verification and biometric checks. Operator intervention is triggered only as a fallback in the event of a data mismatch.

The process is initiated by the Applicant via authentication with pre-existing electronic identification credentials that meet a significant level of guarantee, such as SPID Level 2 for Italian applicants. This method is considered an entry factor to the identification procedure.
Following authentication, a short real-time video of the identity document is requested, which must be physically in the possession of the Applicant. The document must be correctly framed to allow the system to accurately capture and verify both the front and back.

The scanned document is subjected to OCR technology which automatically extracts the personal data contained in the document itself; specific checks on MRZ are also carried out. The system performs a cross-validation with the eID data.

Additional checks carried out by the system are:

- Verification of image quality;
- Validation of the security elements of the document;
- Comparison of the template with a database of documents;
- Use of fraud detection algorithms.

Once this first phase has been completed, passive **liveness detection** is performed to verify that the person presenting the identity document is physically present and is not

trying to deceive the system through photographs, videos or deepfakes. The mechanism works by analysing specific biometric signals acquired during a short video session from which a selfie is extracted, without requiring active user interaction. This stage is crucial to confirm that the individual is the rightful holder of the document.
A biometric comparison is made between the captured selfie and the facial image previously extracted from the identity document. This face matching process is conducted using biometric algorithms (1:1 comparison) that calculate a reliability score representative of the degree of similarity between the two images.
If the score reaches or exceeds the defined threshold, the comparison is considered successful; otherwise, an operator is quickly involved in performing the manual verification. Results are delivered in less than 5 minutes.

Scenario	General condition	Action
Approved (Automatic)	All checks passed with no discrepancies in data	User identity verified, process completed without operator intervention
Approved (Manual)	Data discrepancy resolved with carrier approval	User identity verified after carrier review
Rejected	Checks failed OR unresolved discrepancy OR operator refusal	User identity not verified, process terminated

Figure 6: Use Case Scenario – eID LoA sub and ID Self Fast

The evidence managed in this flow is:

- eID assertion (contains the personal data of the eID holder);
- Images (and videos) of the identity document;
- Data extracted from the identity document;
- Biometric data (image and video of the user's face);
- Your contact information;
- Procedural logs with operator controls (if any) and IDSelf actions.

4.2 Identification with *eID LoA high*

This identification flow involves fully automated onboarding and makes use of authentication via high-level national electronic identity tools (eID Level 3 eIDAS). Neither the acquisition of the identity document nor the biometric verification is required, let alone the intervention of an operator.

The process is initiated by the Applicant via authentication with pre-existing electronic identification credentials that meet a high level of guarantee, such as CIE Level 3 for Italian applicants.

The process is highly efficient, as it is supported by **digital identity federation** allowing authentication between systems seamlessly. High-level authentication allows the secure transfer of the Applicant's personal data to the system, through interaction with authoritative sources, such as CIE Level 3 databases. This direct connection significantly reduces manual entry, minimizes the risk of errors, and ensures the accuracy of identity data from the start.

With this type of authentication, the identity verification process is considered to have been successfully completed and complies with the applicable assurance requirements.

Scenario	General Condition	Action
Approved	eID authentication Level 3 successfully completed	Identity verified, Job completed automatically
Rejected	eID authentication failed o Invalid eID level	Unverified identity, Process Terminated

Figure 7: Use Case Scenario – eID LoA high

The evidence managed in this flow is:

- eID assertion (contains the personal data of the eID holder);
- Your contact information;
- Procedural logs.

4.3 Identification with *ID Self Trust*

This identification flow uses ID capture, biometric verification with liveness detection, and **mandatory operator review** in all cases.

The process begins with the acquisition of the Applicant's identity document. This initial step ensures that the document is in the possession of the applicant, is valid and authentic.
The document must be clearly framed in real time, to allow accurate capture and verification by the system (front and back). The scanned document is subjected to OCR technology that automatically extracts essential personal information; specific checks are carried out on the MRZ.

Next, the system performs **passive liveness detection** to verify that the person presenting the ID is physically present and is not trying to trick the system. The system analyses the biometric signals acquired during a short video session, without requiring active user interaction.

Subsequently, the intervention of an experienced back-office operator is mandatory, to review and verify the correct sampling of the document.

Below is an overview of the checks performed by the operator:

- validation of the data extracted from the identity document, ensuring consistency and accuracy;
- validation of the MRZ, to verify its integrity and confirm that the information corresponds to the data printed on the document;
- verification and confirmation of the facial comparison;
- closing the request with production of the final report

Back-office operators carry out manual verification operations 24/7, the results are available in less than 5 minutes.

Scenario	General Condition	Action
Approved	All checks passed and additional operator approval	User identity verified, process completed
Rejected	Failed checks or refusal by the operator	User identity not verified, process terminated

Figure 8: Use Case Scenario – Self Trust ID

The evidence managed in this flow is:

- Images (and videos) of the identity document;
- Data extracted from the identity document;
- Biometric data (image and video of the user's face);
- Your contact information;
- Procedural logs with operator controls and Self ID actions.

4.3.1 Identification with *ID Self Trust (with challenge)*

This identification process includes all the advanced controls described in the previous paragraph, with the addition of **challenges.** Active challenges consist of the request for specific random actions or movements from the Applicant side. The correct execution of these random actions is verified by biometric analysis and temporal correlation, in order to prevent replay attacks, spoofing, deepfakes and video injection.

Scenario	General condition	Action
Approved	All checks passed, active challenge successfully completed and operator approval	Verified user identity with high IAD certification level
Rejected (Automatic)	Active challenge not passed or inactivity detected, or non-compliance of movements	Process terminated, user notified
Rejected (Operator)	The operator identifies indicators of fraud or operator rejection following review	User identity not verified, process terminated

Figure 9: Use Case Scenario – Self Trust ID with Challenge

4.4 Identification with *ID Doc, NFC technology and Face ID*

This identification process involves an advanced onboarding workflow that combines ID capture, NFC chip reading in electronic documents, and facial biometric verification. Operator intervention is triggered only as a fallback in cases of mismatch or insufficient reliability of the face matching result.

The process is based on a digital identity document and is structured in compliance with the eMRTD standard (ICAO Doc 9303). The process begins with the acquisition of the MRZ of the identity document, from which the access key (BAC or PACE key) is derived. This key allows secure communication to be established with the chip embedded in the document, compliant with ICAO standards, from which the holder's identifying attributes, including the facial image and other personal data contained in the document, are acquired.

The authenticity and integrity of the data extracted from the chip is verified through passive authentication, ensuring that the document has been issued by a recognized authority and has not been altered.

Next, the Applicant is asked to perform a passive *liveness detection* sequence via the device's camera. A representative frame is automatically extracted from the captured video stream, which is compared with the facial image obtained from the eMRTD chip using face matching algorithms.
The positive feedback between the two images allows to establish a secure and reliable binding between the physical presence of the Applicant and the identity attributes extracted from the electronic identity document.

If the score reaches or exceeds the defined threshold, the comparison is considered successful; otherwise, an operator is quickly involved in performing the manual verification. Results are normally delivered in less than 5 minutes.

Scenario	General condition	Action
Approved (Automatic)	All checks passed and facial comparison successful	User identity verified, process completed without operator intervention
Approved (Manual)	Facial discrepancy resolved with operator approval	User identity verified after carrier review
Rejected	Failed checks or failed NFC authentication, or unresolved discrepancy, or operator rejection	User identity not verified, process terminated

Figure 10: Use Case Scenario – Doc ID, NFC, and Face ID

The evidence managed in this flow is:

- Images (and videos) of the identity document;
- Data extracted from the identity document;
- Biometric data (image and video of the user's face);
- Data extracted from the NFC reading of the document, including the image of the holder's face;
- Your contact information;
- Procedural logs with operator controls and actions DOC ID/FACE ID/NFC ID

4.5 Identification with *Namirial Wallet*

The EUDI Wallet can be understood as a secure digital container that allows users to securely store and manage personal or organizational data directly on their devices (mobile or web-based). This innovative solution is part of the European Commission's ongoing efforts to strengthen the security, privacy protection and interoperability of digital identities between EU Member States.

This identification flow involves fully automated onboarding, neither document capture nor biometric verification is required, nor the intervention of a back-office operator. The applicant opens the Digital Wallet app, scans the QR code, or follows the deep link, and authorizes the presentation of the PID credential.

Namirial Wallet includes a **personally identifiable information (PID),** issued on the basis of an enrollment and identity verification process performed by Namirial pursuant

to the previous paragraphs and consistent with the draft FprCEN/TS 18098 of July 2025, linked to a key pair stored securely on a certified remote HSM. The Wallet Secure Cryptographic Device (WSCD) complies with assurance level AVA_VAN.5 and is based on a Common Criteria certified HSM module with EAL4+ level. It grants the user exclusive control over the key pairs associated with the Wallet Unit.

Namirial Wallet serves as the equivalent of a LoA High level eID tool, used for strong and continuous authentication of the identity previously verified by Namirial.
The Wallet is used exclusively for the provision of digital identity and trust services provided by Namirial or contractual partners operating in the Namirial ecosystem of services. Consequently, the Namirial Wallet does not constitute an electronic identification (eID) scheme notified under Article 9 of the eIDAS Regulation, but a credential and a proprietary scheme with a high level of trust.

The system receives and validates the PID from the user's Wallet; the process ends immediately after the successful Wallet authentication and PID validation.

Scenario	General condition	Action
Approved	Successful Wallet authentication, successful PID validation, and all valid cryptographic proofs	User identity verified with high assurance level, process completed automatically
Rejected	Wallet authentication failed or invalid/expired PID credential, or failed signature verification, or revoked credential	User identity not verified, process terminated with error code

Figure 11: Use Case Scenario – Namirial Wallet

After enrollment, the Wallet and Namirial PID are used to authenticate the applicant for multiple purposes, including the issuance of qualified digital certificates.

The evidence of managed enrollment is:

- PID (Verifiable Presentation) assertion contains personal data with a high level of assurance (surname, first name, date of birth, place of birth, nationality, unique identifier);
- Cryptographic proofs: JWT signatures, certificate chains, nonce values;
- Contact Information: verified email address and phone number;
- Procedural Logs:
    - OID4VP authentication flow events
    - Timestamps for all critical steps
    - About the Wallet Provider

- Information about the PID issuer
- User consent records
- Session security parameters

5 CONTROLS AND SECURITY MEASURES

5.1 Physical security checks

Namirial has implemented an Information Security Management System (ISMS) in line with the international standard for information security ISO/IEC 27001.
It also operates for all delivery sites, in accordance with its SCS-P05 Group Information Security Operational Policy, designed to detect, deter and prevent unauthorized access to the Organization's operations.

In the context of the provision of the service covered by this document, the information security measures are consistent with the certifications obtained.

5.1.1 Physical access

These measures apply to the facilities from which the service is provided, in their respective production and contingency environments, which are periodically audited in compliance with applicable legislation and Namirial's internal policies.

5.1.1.1 Site Location

Production data centers are managed by:

- Amazon AWS, in Ireland, Dublin: ISO 27001, SOC 1/2/3 and PCI DSS certified);
- FreePro, in France, Marseille and Lyon: ISO 27001 / PCI-DSS / HDS certified and with an ongoing SecNumCloud qualification process.

These certifications ensure that both sites adhere to rigorous security controls and risk management processes.

5.1.1.2 Physical access controls

The facilities through which the service is provided are redundant and protected by measures that prevent unauthorized access to and disclosure of data.
Physical protection is achieved through the implementation of clearly defined security perimeters around the service, such as anti intrusion systems with barriers around the building and reinforced security doors.
Three levels of access control are implemented, to be achieved progressively, including biometric detection (fingerprint reader).
Access is strictly limited to expressly authorized personnel, who must be identified at the entrance and registered. The system automatically records inputs and outputs.

In addition, active anti-intrusion systems, such as alarm systems and constant video surveillance of indoor and outdoor spaces.
The facilities have preventive and corrective maintenance systems with 24-hour assistance, 365 days a year, and interventions within 24 hours of reporting.

5.1.2 Electrical system and air conditioning

The rooms that house the IT equipment are equipped with a highly secure and redundant electrical infrastructure, including power stabilization systems and dual power supply with generator. The entire configuration ensures continuous energy availability, with N+2 redundancy. The facility also has advanced temperature control systems.

5.1.3 Fire prevention and protection

Major data center (DC) infrastructure and assets are equipped with automated fire detection and extinguishing systems.

5.1.4 Flood protection

The structures are located in an area with a low risk of flooding. The rooms that house the computer equipment are equipped with a humidity detection system and sensors that detect the presence of liquids and activate an alarm in the event of flooding.

5.1.5 Media handling

Your assets are protected from accidental damage and unauthorized physical access. Only authorized personnel have access to management and storage media. Highly confidential information is stored securely in an external safe.
The removal of supports, both paper and magnetic, is carried out by means of mechanisms that guarantee the irretrievability of the information.

5.2 Procedural controls

All procedures related to security in the provision of the service, including the identification and verification of specific attributes for the issuance, management and use of qualified electronic signature certificates, are carried out by Namirial's trusted personnel. A sufficient number of qualified employees is always guaranteed to ensure compliance with applicable legislation and internal policies and procedures.

5.2.1 Trusted roles

The trusted roles provided for by the ETSI EN 319-401 standard are named, they possess the necessary experience, professionalism and technical expertise. They also receive the necessary level of training on the procedures and tools that can be used in the various operational phases.

All personnel appointed according to trusted roles must be free from conflicts of interest that may be detrimental to the level of impartiality in the operations carried out by each in the performance of his or her duties.
Trusted roles are appointed by management. A list of the personnel appointed in these roles is maintained and reviewed by the Organization, in a special document of Organizational Structure, which is maintained and revised by Namirial, as well as sent to the Supervisory Body with each update.

5.3 Personnel controls

All personnel involved in the provision of the service have adequate experience in the definition, development and management of the service and receive, on a regular basis, the necessary level of training on procedures and tools that can be used in various operational phases.

Namirial staff in charge of these activities must:

- possess the necessary competence, reliability, experience and qualifications and have received training relating to security and personal data protection rules appropriate to the services offered and their job function;
- be able to meet the requirement of "knowledge, experience and qualifications" through actual training or experience, or a combination of both;
- be up-to-date on new threats and the latest applicable security practices.

Namirial hires staff with the highest levels of integrity and expertise. There is no citizenship requirement for the staff involved in the provision of the service.

5.3.1 Background check

Namirial verifies the identity and performs a check of the previous experience of each employee in order to assign one of the trusted roles provided and indicated above

5.3.2 Check of ongoing experiences

The company's Human Resources function, with the support of the Service Managers, implements a process of continuous monitoring of staff skills and performance. The process involves the assignment of specific objectives defined according to the role held, as well as the periodic monitoring of progress and the percentage of achievement of the same.
To support this monitoring, the Service Managers organize periodic one-to-one meetings with the resources of their team, aimed at verifying the adequacy of the skills with respect to the assigned role and intervening promptly in the event of deviations or the need for reinforcement.

The continuous analysis of skills also makes it possible to assess the correct allocation of resources and to define annual training programs, aimed at filling any gaps that have emerged and strengthening staff awareness of policies and procedures relevant.
Through these safeguards, Namirial ensures that the resources involved in the provision of services are constantly monitored over time and maintain an adequate level of competence

5.3.3 Training Requirements

Namirial staff receive basic information security training and data protection awareness early in the corporate onboarding process. This training is subsequently re-proposed on a regular basis (at least annually) through the administration of video lessons, accompanied by special learning tests.

The compulsory courses include, in particular, the following subject areas:

- GDPR and Data Protection (selected by the DPO)
- Security Awareness (selected by the CISO)

The functions responsible for verifying training (Human Resources, DPOs, CISOs and Business Unit Managers) have tools for analysing and monitoring the status of completion of the training courses, mentioned above, by staff. In addition, dedicated on-the-job training is provided to all Namirial personnel involved in specific tasks, as described in this document.

5.3.4 Training update frequency and requirements

Staff are expected to maintain high levels of competence through industry-relevant training sessions in order to continue to act in accordance with the requirements of their role.

At the beginning of each year, training needs are analysed to define the courses to be delivered. The analysis is based on the following steps:

- Meeting with the company management to collect data on the training needs necessary to achieve the objectives.
- Feedback from business unit managers to identify the specific training needs of each department.
- Presentation of the data collected to the company management for the finalization and approval of the Training Plan.

Once defined, the Training Plan is shared with all staff at the beginning of the year.

5.3.5 Frequency of job rotation

In the event of role rotation, Namirial performs a security audit, including a verification of credentials at the level of networks, systems, applications or other resources used, as well as access permissions to facilities and areas.

5.3.6 Requirements for non-employee personnel

Non-employee staff are subject to the specific requirements and obligations of the role, as well as the related sanctions.

5.3.7 Documentation provided to staff

Onboard personnel are provided with the information necessary to perform their duties, including a copy of this document and the operational documentation necessary to maintain the integrity of operations.

5.3.8 Penalties for unauthorized actions

Namirial personnel who do not comply with the organization's internal policies and provisions, whether through negligence or wilful misconduct, are subject to administrative or disciplinary sanctions, including termination of employment or collaboration and, in the most serious cases, criminal sanctions.

5.4 Procedures for audit logging and record archive

The events generated by the system produce logs, which allow tracing the different operations that occur during the automatic and user interaction processes, facilitating the diagnosis of any anomalies and/or incidents

5.4.1 Types of logged events

Namirial produces and maintains records of at least the following events related to the security of the system:

- Activating and shutting down the system;
- Maintenance and changes of system settings;
- Attempts to create, delete, set passwords, or change privileges;
- Changes related to the management of privileged accounts;
- Attempts at unauthorized access to systems through the network;
- Unauthorized access attempts to the file system;
- Log access;
- Records of the destruction of media, including those containing cryptographic keys and activation data;
- Cryptographic module lifecycle events;
- The key generation ceremony and the key management databases;

- Physical access logs;
- Complete reports of attempts at physical intrusion into the infrastructures that support the service;
- Reports of compromises and discrepancies;
- Watch synchronization and recalibration events

With reference to the Onboarding process, the events collected and recorded are:

- Personal data of the applicant;
- Photograph of the front of the identity document;
- Photograph of the back of the ID;
- Photograph of the face extracted from the identity document;
- Face photograph extracted from biometric video;
- Original Biometric Video;
- Original video of the ID document.

Audit and logging information:

- Audit trail
- Operator activity logs, which should include:
    - Full name of the operator
    - Operator User ID
    - Evidence of actions performed with time references
    - Who performed the action, what action, when and for how long
- Logs containing the versions of all modules involved

The logs include the following:

- Date and time of the event;
- Serial number or sequence of the event, in the automatic logs;
- the user who performs the event;
- Type of event.

5.4.2 Log storage and processing frequency

The processing of the logs consists of their periodic review, aimed at verifying their integrity and analyzing the recordings present, with particular attention to alerts or anomalies. Any further investigations and consequent actions are formally documented.

Namirial maintains a system that allows it to guarantee:

- sufficient space for storing logs;
- that log files are not overwritten;
- that the saved information includes at least: event type, date and time, user performing the event, and result of the operation.

Log files are stored in structured files that can be embedded in a database for later exploration.

The frequency of saving the audit log is daily. The time used to log events must be synchronized with UTC at least once a day.

5.4.3 Record archive

Namirial produces and maintains accessible records that include all relevant activities and information related to the data issued and received by Namirial. The QTSP procedure requires that events detected and available in the database are extracted and placed in managed text files to ensure their integrity and availability.
The evidence generated during the identity verification process is stored in a tamper-proof manner, ensuring the confidentiality of the information. The evidence is stored in Namirial's Long-Term Archiving (LTA) system.
If the onboarding process is used for the issuance of qualified electronic signature certificates, the data and evidence are stored for 20 (twenty) years, in accordance with Italian legislation.
The records relating to the operation of the services are made available to the judicial authority in the event of legal proceedings and, internally, for the purpose of periodic audits and verifications of the system.
These registers remain accessible even in the event that Namirial has ceased its activities.

5.4.4 File protection

The files are protected in such a way that only duly authorized personnel can access them. They are safeguarded from viewing, modification, deletion or any other form of tampering, as they are stored within a trusted system. Namirial ensures adequate protection of files by assigning qualified personnel to process them and storing them in secure external facilities.

5.4.5 Backup procedures

Namirial has an appropriate backup procedure in place that ensures that in the event of loss or destruction of the relevant files, the corresponding backup copies of the logs are available within a short period of time.

5.4.6 Log storage system

Log information is collected internally and automatically by the system, network communications and service software, as well as any manually generated data, which will be stored by duly authorized personnel.

5.4.7 Notification of the audit event to the event causator

When the log storage system logs an event, you don't need to notify the person, organization, device, or application that caused the event.

5.4.8 Vulnerability analysis

Namirial periodically performs vulnerability assessment and penetration testing activities on its systems, respecting the deadlines indicated by the reference standards.
Based on the results obtained, all necessary countermeasures are implemented to ensure the security of applications and systems.

5.5 Information storage

Appropriate registers are drawn up and stored for each relevant event.

5.5.1 Types of Archived Logs

The CA retains all information relating to:

- all data related to the lifecycle of the onboarding process;
- requests for identification;
- identity documents presented at the time of the identification request;
- personal data of the Applicant;
- audit trail;

5.5.2 Storage period

These records are kept for a period of 20 years.

5.5.3 Archive protection

Namirial protects the archives through physical and logical access controls, so that only duly authorized persons can access them. The archive is protected from viewing, modification, deletion or any other manipulation thanks to the implementation of a reliable system.

5.5.4 Archive backup

All information subject to storage is subject to increased backup procedures to the DR site, in order to ensure its availability, integrity and recoverability in the event of an incident or unavailability of primary systems.

5.5.5 Date and time

The logs are dated with a reliable source via NTP. This information does not need to be digitally signed.

5.5.6 Recording storage and retention system

The recording archiving and retention system is managed internally by Namirial through a compliant storage system, compliant with the applicable regulatory and security requirements.

5.5.7 Procedures for obtaining and verifying storage information

The stored information shall be made available through specific procedures for verifying and making available that information

5.6 Incident Management procedures

Namirial has developed security and business continuity policies that enable the management and recovery of systems in the event of incidents and compromise of its operations. The specific procedure for managing and responding to incidents, also applied through an alert system and the generation of periodic reports, is described in detail in the appropriate internal documentation at Namirial.

5.6.1 Corruption of assets, applications, or data

When an asset, application, or data corruption event occurs, appropriate management procedures are followed in accordance with Namirial's security and incident management policies, which include escalation, investigation, and incident response. If necessary, key compromise or disaster recovery procedures in Namirial are triggered.

5.6.2 Business continuity

Namirial will restore critical services in accordance with the business continuity plan related to the service, restoring the normal operation of previous services within a maximum of 24 hours after the disaster.

5.7 Termination Plan

Namirial has established an updated termination plan for the service covered by this document, which will be implemented if the need arises.

The document contains the following provisions:

- Provision of the necessary funds, including liability insurance, to perform the cessation activity;
- communication to the Supervisory Authority, to all subscribers of the service, to Third Parties and in general to any third party with whom you have agreements or other types of relationship with a minimum of 3 (three) months in advance;
- performing the activities necessary to transfer the obligations to maintain log information and evidence for the respective time periods.

6 TECHNICAL SECURITY CONTROLS

6.1 Use of cryptography to subscribe to the evidence of the identification process (*audit trail*)

The evidence of the identification process (audit trail) is protected by cryptographic mechanisms that guarantee its authenticity, integrity and immutability over time.

To this end, each audit trail is signed with a qualified electronic seal of the QTSPNamirial, in accordance with the eIDAS Regulation. The qualified electronic seal is based on a qualified certificate and a cryptographic key pair (private key and public key).

The use of cryptography is therefore a fundamental technical element to ensure the evidentiary value of audit trails and their reliability over time.

6.2 Cybersecurity controls

The instrumentation used is configured with the appropriate safety profiles, by Namirial systems personnel, in the following aspects:

- operating system security configuration;
- application security settings;
- correct sizing of the system;
- configuration of users and permissions;
- configuring log events;
- backup and recovery plan;
- network traffic requirements;
- technical life cycle controls;
- controls on the Development of the System.

The operating systems used by Namirial for the management of the provision of the service have a high level of security and follow the hardening procedures established by Namirial. Tasks and areas of responsibility are segregated in order to minimize the possibility of unauthorized modification or misuse of Namirial's resources.

System access events are logged; the components of the local network are maintained in a secure environment, and the configurations are periodically checked for compliance with the requirements specified by Namirial.
Automated jobs are implemented to verify the integrity of the software and its configuration.
Continuous monitoring and alerting systems are implemented to allow Namirial to detect, record and respond promptly to any unauthorized and/or irregular attempt to access its resources.

6.3 Network security controls

Namirial's network architecture is structured on several levels in order to create separate network environments, addressed to hosts related to different functions and characterized by different levels of criticality.
The security of access and network traffic is guaranteed through the application of protection policies implemented on firewall systems located on different network levels. Requests to implement new firewall rules are handled through a change request.
The activation of rules that cause a high level of impact is dealt with with the Security Officer. Private network security is accomplished not only by the perimeter protection systems described above, but also by a specific configuration that keeps internal addresses as confidential. Communications between management stations and systems are protected by means of tools that ensure authentication between parties and their privacy.
Potential remote connections take place over an encrypted VPN channel and require authentication (MFA) via username, password, and an authentication token (OTP). Communication between the application modules of Namirial's PKI platform takes place through cryptographic channels.
Communication between users accessing online services takes place through TLS/SSL connections with SHA -256 algorithm.
The system implemented to manage user access provides both AAA (authentication, authorization, access) and profiling mechanisms and encryption of the communication channel with TLS/SSL protocol

7 AUDIT AND COMPLIANCE

Namirial is a Qualified Trust Service Provider subject to periodic service conformity assessment activities by a Conformity Assessment Body (CAB), recognized in the EU.

Namirial is also subject to a conformity assessment ("surveillance") by the AgID Supervisory Body

7.1 Frequency and circumstances of conformity assessment

Namirial's audit function is responsible for internal audits of the service covered by this document, which is responsible for verifying that the processes comply with legal requirements, the eIDAS Regulation as well as the technical standards governing the provision of the service. The internal audit is carried out at least once a year.

The third-party audit, likewise, is carried out by a Conformity Assessment Body at least annually.

7.2 Actions arising from non-conformities

In the event of non-compliance, Namirial takes the necessary corrective actions by establishing a resolution deadline that is appropriate to the nature and criticality of the same. The progress of corrective activities is monitored until they are completely closed.

If the Supervisory Body detects any non-compliance with the requirements of the eIDAS Regulation (EU), Namirial will take all necessary corrective measures within the deadlines indicated by the competent Authority.

7.3 Reporting results

The results of the audits are shared with Namirial through a conformity assessment report. The result of the internal audit, on the other hand, is communicated to the Management and to the Head of the Service, in charge of providing the service itself.

8 LEGAL AND BUSINESS ASPECTS

8.1 Rates

The fees for NOB services are governed by the commercial agreement between Namirial and the Partner. No fees are defined herein.

8.2 Financial responsibility

Namirial has sufficient financial means to maintain its operations and fulfil its obligations, as well as to address the risk of liability for damages, as set out in ETSI EN 319 401, in connection with the management of the termination of services and decommissioning plan.

8.3 Insurance coverage

Namirial has taken out professional indemnity insurance which includes the qualified trust services described herein. The policy is publicly available on the Namirial website at the following link https://www.namirial.com/it/documentazione/

The specific limits of insurance coverage applicable in the relationship with Partners are defined in the Addendum.

8.4 Protection of personal data

Personal information concerning Service Applicants and, more generally, customers of the service provided is processed, stored and protected in accordance with the provisions of European Regulation 679/2016 on the protection of personal data.
Namirial S.p.A. guarantees the protection of data subjects, in compliance with European Regulation 679/2016 on the protection of personal data. In particular, it provides the interested parties with all the necessary information, in relation to the right of access to personal data and the uses of the same, permitted by law.

8.4.1 Data Controller

The controller of personal data is:

- Namirial S.p.A.
- VAT number: IT02046570426.
- Address: Via Caduti sul Lavoro n. 4, 60019 Senigallia (An) - Italy.

The terms and conditions applicable to the processing of personal data, including the division of responsibilities between the Parties, are governed by the Data Processing Agreement (DPA), entered into pursuant to Article 28 of the GDPR and annexed to the Partner Addendum.

8.4.1.1 Contact details of the organisation responsible for data protection

The contact details of the Data Protection Officer are:

- Website: https://www.namirial.com/it/privacy-policy/
- E-mail: dpo@namirial.com
- PEC: dpo.namirial@sicurezzapostale.it

8.4.2 Type of data processed

As part of the identification and onboarding service, the following categories of personal data are processed:

- Personal data (name, surname, tax code, gender, date of birth, place of birth, nationality);
- Details and copy of identity document;
- Address data (residence/domicile);
- Contact details (telephone number and e-mail address);
- Biometric data (physical, physiological or behavioural characteristics collected through photo/video recognition);
- Browsing data and logs (IP, connection data, domain names and other parameters relating to the operating system and browser you use).

8.4.3 Purpose of the processing

Personal data are acquired in compliance with the purposes set out in the information provided to the Applicant during the certificate request phases. The information is also published on https://www.namirial.com/it/documentazione/, in the specific Privacy Policy section.

The purposes of the processing are listed below.

- Provision of the service: the data is collected through an appropriate contract and is processed in order to provide the electronic services requested by the users, as described in this document;
- Conclusion of the contract and use of services:
- Verification of the identity of the data subject through photo/video recognition;
- Consent; Management and response to requests for technical assistance, including online Fulfilment of legal, national or EU regulatory obligations;
- Sending information with informational content
- Statistical, business and market analyses, carried out in an absolutely anonymous and aggregate form;
- Judicial protection of Namirial rights;
- Prevention of fraudulent activities by carrying out a check on the reliability of the data provided by the data subject at the time of recognition.

8.4.3.1 Privacy Policy and Consent

Personal data are acquired in compliance with the purposes set out in the information provided to the Applicant during the certificate request phases. The information is also published on https://www.namirial.com/it/documentazione/, in the specific Privacy Policy section.
The privacy policy is presented to the Applicant before the start of the identification session. The mechanism for acquiring explicit consent to the processing of biometric data pursuant to Article 9 of Regulation (EU) 2016/679 (GDPR), as well as the methods for recording it within the audit trail, are governed by the Prtner Addendum.

8.4.4 Processing methods

All personal information, acquired during the provision of services, is processed by Namirial in accordance with the GDPR, adopting the appropriate security measures described in this manual in order to prevent its loss, avoid unlawful use or access by unauthorised personnel.

The data in electronic format are stored in special data servers used for this purpose and on optical media in protected cabinets. Namirial S.p.A. reserves the right to store paper data at its headquarters, in protected paper archives that can only be accessed by expressly authorized appointees

8.4.5 Other forms of data use

Personal data may be used for purposes other than the provision of the services described in this manual and may be communicated to public bodies, such as law enforcement, public authorities and judicial authorities, if the same subjects request it for reasons of public order and in compliance with the provisions of the law for the security and defense of the State, the prevention, detection and/or repression of crimes.

More information can be found at https://www.namirial.com/it/privacy-policy

8.4.6 Data retention

Evidence of identity verification is retained by Namirial for the period agreed with the Partner and specified in the Addendum. If the NOB session concludes with the issuance of a qualified certificate, the evidence shall be retained for at least 20 (twenty) years from the date of issue, regardless of what is stated in the Addendum.

8.4.7 Data transfer

Personal data will not be transferred to third parties, except in the following cases:

- when required by applicable law;
- where there is a legitimate interest;
- to comply with a request from the competent judicial or administrative authority;
- in the event of termination of the service.

Namirial does not make international data transfers outside the EU or EEA. Onward transfers by the Partner to third parties are subject to the Partner's data protection obligations.

8.5 Intellectual Property Rights

This document is the property of Namirial S.p.A., which reserves all rights. As regards the ownership of other data and information, the regulations in force apply.

8.6 Obligations, warranties and responsibilities

8.6.1 Obligations of the IPSP

Namirial, as IPSP, is required to:

- operate in accordance with this Operating Manual and applicable regulations, as well as the ETSI TS 119 461 standard;
- comply with the requirements of the applicable legislation on identity verification;
- identify with certainty the Applicant undergoing onboarding;
- verify the authenticity of the onboarding request;
- issue and manage identity verification evidence;
- record and store the evidence relating to each identity verification, with a date and

time certified by a qualified time reference;
- electronically preserve all evidence for the periods specified herein;
- provide a copy of this Operating Manual to anyone who requests it;
- take secure measures for the processing of personal data in accordance with the GDPR;
- comply with all obligations arising from the Data Processing Agreement entered into with the Partner.

8.6.2 Obligations of Applicants

In all cases, the applicant is required to:

- provide all the information requested and guarantee its truthfulness and reliability;
- provide, with explicit consent, the collection of the data required for identification;
- present a valid identity document that meets the requirements set out in this document;
- not attempt to circumvent or impair the identification process;
- promptly notify you of any change in the information and circumstances stated at the time of identification.

8.6.3 Obligations of the Relying Party

The relying party using NOB identity verification evidence is required to:

- ensure that the IPSP or TSP is certified or demonstrates compliance with ETSI TS 119 46;
- ensure that identity verification evidence or identity attributes come from a trusted and trustworthy source;
- clearly define expectations and how the verified data will be used;
- refrain from using the service for illicit purposes or in any way contrary to the applicable contractual provisions;
- keep constantly updated and adequate all the resources necessary for the correct use of the service.

Additional obligations of the relying party are specifically defined in Addendum, Section C.

8.6.4 IPSP Guarantees

The IPSP ensures that the identity proofing process is carried out in accordance with the applicable requirements of ETSI TS 119 461 and applicable regulations, ensuring that appropriate technical and organisational measures are in place for the correct verification and binding of the Applicant's identity. The IPSP also ensures the traceability of the operations carried out and the storage of the evidence necessary to support the level of assurance declared for the identification process.

8.6.5 Relying party guarantees

The Relying Party warrants that it will use the information and identity attributes received only for the permitted purposes and in compliance with the applicable terms of use and applicable law. The Relying Party also ensures that it carries out the necessary checks to assess the reliability of the data received, in accordance with the declared level of assurance and the applicable validation rules, taking responsibility for decisions based on such information.

8.6.6 Applicant's guarantees

The Applicant warrants that all information, data and documents provided as part of the identification process are true, complete, accurate and up-to-date. The Applicant also guarantees that he/she is entitled to request the activation of the service and the issuance of any associated certificates or credentials, as well as to use the service in compliance with the applicable regulations and contractual conditions.

8.6.7 Applicant's responsibilities

The Applicant is responsible for the correctness, completeness and up-to-date nature of the information and data provided as part of the identity proofing process.
The Applicant is responsible for all actions carried out using its credentials or authentication tools, except in cases of unauthorized use not attributable to negligence or wilful misconduct.
The Applicant is also responsible for promptly reporting any event that may compromise the security of the identification process or the validity of the verified identity.

8.6.8 Disclaimer of warranties

Except as provided for by applicable law, the Terms of Contract and the provision of this document, Namirial does not provide any further guarantees than those expressly indicated in the contractual documents.

8.6.9 Limitation of liability

Namirial is not responsible for delays, errors or non-fulfilment attributable to third parties, nor for anomalies in the provision of the service beyond its technical control, including, but not limited to, malfunctions of telecommunications or telematic networks.

Namirial is also not responsible for:

- incorrect, incomplete or false information provided by the Applicant;
- misuse of the service by the Partner or its Applicants;
- decisions taken by the Partner or by third parties solely on the basis of the outcome of the identity verification process;

- unavailability of the service due to scheduled maintenance activities or unexpected technical malfunctions.

Namirial's liability is limited only to cases in which there is evidence of a material breach attributable to intent or gross negligence.

Namirial is not liable for indirect, consequential, loss of profit, loss of data or other damages not directly attributable to a breach of the same.

Liability remains unaffected for mandatory obligations under applicable law, including trust services and personal data protection regulations.

8.6.10 Allocation of responsibilities and compensation

The allocation of liabilities between Namirial and the Partner — including the applicable insurance coverage limits in the *B2B* relationship and any indemnification obligations is governed solely by the Partner Addendum.

8.7 Indemnification and Indemnification Limitations

Namirial is indemnified and held harmless from any claim, damage, loss or cost (including reasonable attorneys' fees) arising from breaches of contractual or regulatory obligations not attributable to Namirial, including the non-compliant use of the service or the provision of inaccurate, incomplete or outdated information. The obligation to pay compensation does not apply to the extent that the damage is caused by intent or gross negligence on the part of Namirial.

8.8 Terms and Termination

The provisions of this document apply from the date of the user's subscription to the Onboarding service, made available by Namirial, and are considered fully accepted.

8.9 Dispute resolution procedures

Any complaints or reports may be submitted through the appropriate channels made available by Namirial, in accordance with the procedures set out in the internal complaints handling procedure.

Namirial ensures the timely handling of complaints received and their management according to criteria of traceability, transparency and fairness, providing feedback within the deadlines provided for by the applicable procedure

8.10 Terms and Conditions

The Terms and Conditions presented to applicants prior to the start of the NOB session and the mechanism by which acceptance is recorded are defined in the Partner Addendum.

Namirial's Terms and Conditions exclusively govern the B2B business relationship between Namirial and the Partner, as defined in the commercial agreement.

8.11 Place of jurisdiction

For all disputes arising from this Operating Manual, from the Terms and Conditions accepted by the Applicant or from any other contracts stipulated for the use of the services made available by Namirial, the Court of Ancona will have exclusive jurisdiction.

8.12 Applicable law

The provision of the service and the stipulation of contracts are subject to Italian law and as such will be interpreted and executed. The service is provided in accordance with Italian law, the eIDAS Regulation and the ETSI TS 119 461 standard.