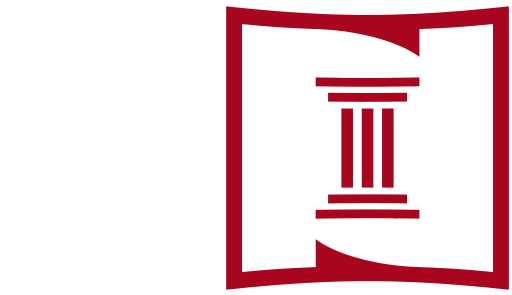


InfoNotary

POLICY AND PRACTICE FOR THE PROVISION OF A NATIONALLY QUALIFIED REMOTE VIDEO IDENTIFICATION SERVICE

OF THE QUALIFIED TRUST SERVICE PROVIDER
INFONOTARY PLC

Version 1.2

Effective from 16.12.2024 г.

TABLE OF CONTENTS

1. INTRODUCTION

The main purpose of this document, POLICY AND PRACTICE FOR THE PROVISION OF A NATIONALLY QUALIFIED REMOTE VIDEO IDENTIFICATION SERVICE of the qualified trust service provider INFONOTARY AD (INFONOTARY/the Provider), is to describe and make public:

- the conditions and rules implemented and followed by INFONOTARY when providing the Remote Video Identification Service (the Service/RVIS/Onboarding);
- the applicability and limitations in the use of the Service;
- the specific operational procedures followed by INFONOTARY in the provision of the Service;
- the means for ensuring the Provider's compliance — including its reliability and security — with the provisions and requirements of Regulation (EU) No 910/2014 (amendment with Regulation (EU) 2024/1183) and the applicable Bulgarian legislation.

This document complements and must be read in conjunction with the current published versions of INFONOTARY's documents " Certification Practice Statement for Qualified Certification Services" and " Policy for Providing Qualified Certification Services for Qualified Electronic Signature." These documents contain the general terms and requirements for identification procedures, issuance and management of qualified certificates, as well as requirements for security, key pair (private and public) generation and storage, and their applicability. References to the relevant sections of these documents are provided accordingly.

The Policy and Practice for the Provision of the Remote Video Identification Service is a public document and may be amended when necessary. Any changes will be made publicly available to all interested parties at: http://www.infonotary.com.

This document is prepared in accordance with the provisions and requirements of the European and national regulatory documents and standards listed below:

- 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 Regulation/ Regulation (EC) № 910/2014);
- Regulation (EU) 2024/1183 of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards the establishment of a framework for a European Digital Identity;
- Electronic Document and Electronic Trust Services Act;
- Measures Against Money Laundering Act, Article 55(2);
- Regulation for the Implementation of the Measures Against Money Laundering Act, (Article 42);
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation — GDPR);
- ETSI EN 319 401 General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates;

- ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects;
- ETSI TS 119 612 Electronic Signatures and Infrastructures (ESI); Trusted Lists (points 5.5.1.3 (a, b, g)).

International standards and specifications are used in their current and valid versions.

1.1. MAIN PROVISIONS

1.1.1. Trust Service Provider

InfoNotary PLC is a Qualified Trust Service Provider in accordance with Regulation (EU) No 910/2014 and has been granted qualified status by the national Supervisory Authority in compliance with the provisions of Regulation (EU) No 910/2014 and national legislation.

InfoNotary PLC is a commercial company registered in the Commercial Register at the Registry Agency under UIC 131276827. The company's registered office and place of business is in Sofia, 16 Ivan Vazov Street, Contact phone: +359 2 9210857; website: http://www.infonotary.com.

The company operates under the registered trademark InfoNotary.

As a qualified provider, InfoNotary PLC performs the following activities and pro-vides the following qualified trust services:

- Issuance and management of qualified certificates for qualified and advanced electronic signatures and seals;
- Issuance and management of qualified website authentication certificates;
- Issuance and management of qualified electronic time stamps;
- Issuance and management of qualified PSD2 certificates;
- Validation services for qualified certificates, qualified electronic signatures and qualified electronic seals, including:
  - Real-time status verification services for qualified certificates issued by In-foNotary (OCSP);
  - Real-time validation services for qualified certificates, qualified electronic signatures, and qualified electronic seals (InfoNotary Qualified Validation Service - IQVS);
- Qualified services for remote signing/sealing of electronic documents;
- Nationally qualified remote video identification service;
- Nationally qualified trust service for electronic identification, including services for issuance and management of electronic identity means, and dynamic electronic identity authentication.

In carrying out its activities and providing qualified trust services, InfoNotary PLC applies its internally implemented Management System, certified according to ISO 9001:2008 and its Information Security Management System, certified according to ISO/IEC 27001:2013.

1.1.2. Naming and Identification of the Document

The document Policy and Practice for the Provision of Remote Video Identification is named **"InfoNotary Remote Video Identification Service CP_CPS"** and has the following Object Identifier (OID): **1.3.6.1.4.1.22144.3.8.2.**

1.1.3. Applicability, Use, and Availability of the Remote Video Identification Service

The nationally qualified Remote Video Identification Service is applicable in processes requiring registration and/or verification and confirmation of the identity of a natural person — acting either on their own behalf, as an authorized representative of a legal entity or organization, or as a legal representative of a legal entity or organization — and/or for verification and confirmation of the identity of a legal entity.

The service may be used by users/applicants (natural persons acting on their own behalf or as legal/authorized representatives of a legal entity) for trust services (such as issuance and management of qualified certificates, issuance and management of electronic identification means, or for requesting and managing other trust or informational services provided by the Provider). It may also be used by users accessing services of a third party/organization (e.g. qualified trust service providers, financial or insurance institutions, etc.) that has entered into a contract/agreement with INFONOTARY for the use of the service for internal purposes of the legal entity.

The nationally qualified Remote Video Identification Service provided by InfoNotary PLC is a method of verifying and confirming the identity of a natural person and/or the identity of a legal entity, which ensures a level of assurance and reliability equivalent to the physical presence of the applicant.

The equivalent level of assurance has been audited and confirmed by a Conformity Assessment Body in accordance with Article 24(1)(d) of Regulation (EU) No 910/2014 (amendment with Regulation (EU) 2024/1183).

Due to the manner in which the Remote Video Identification Service is currently provided, it is not suitable for use by individuals with visual, hearing, or speech impairments.

1.1.4. Limitations on the Trust Service's Scope

The Remote Video Identification Service must not be used in a manner that violates the confidentiality and security of personal data.

The Provider shall not be held liable for any damages resulting from:

- use of the Remote Video Identification Service beyond the permitted scope and in violation of its intended purpose and application limitations, which will lead to the invalidation of the guarantees provided by INFONOTARY to users and relying parties;
- accidental events of a force majeure nature, including malicious actions by third parties.

1.2. MANAGEMENT OF THE PROVIDER'S TRUST POLICY AND PRACTICE

The trust policy of the Provider is determined by the Board of Directors of INFONOTARY EAD.

All changes, edits, and additions to this Policy are approved by the Board of Directors of INFONOTARY PLC.

New versions of the document are published after approval in the Provider's Document Registry, which is publicly available at: https://www.infonotary.com.

All comments, requests for information, and clarifications regarding this Policy may be addressed to: INFONOTARY PLC, 1000 Sofia, Bulgaria, 16, Ivan Vazov St., e-mail: legal@infonotary.com.

1.3. TERMS AND ABBREVIATIONS

Bulgarian Identity Document	A certifying document issued by the competent authorities of the Republic of Bulgaria for the purpose of individual identification of Bulgarian and foreign citizens.
Qualified Trust Service Provider	A trust service provider that offers one or more qualified trust services and has obtained its qualified status from a supervisory body.
Person identification data	A set of data that is issued in accordance with Union or national law and that enables the establishment of the identity of a natural or legal person, or of a natural person representing another natural person or a legal person.
Identity Document	A physical or digital document issued by a competent and authoritative government source that certifies the identity of the applicant
Authentic Source	Repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person or object and that is considered to be a primary source of that information or recognised as authentic in accordance with Union or national law, including administrative practice.
Applicant/User	A person (legal or natural) whose identity needs to be verified.
Qualified Trust Service	A trust service that meets the applicable requirements set out in Regulation (EU) No 910/2014 (amendment with Regulation (EU) 2024/1183).
Client	A third relying party that uses the remote video identification service to verify the identity of its own users.
Mobile Application InfoNotary SignZone	Specifically developed software by the Provider, intended for the secure delivery and use of the Provider's trust services, published in the respective mobile application stores for the Android, iOS, operating systems.

Remote Video Identification / Onboarding Process	An identity verification process in which the applicant/user is physically remote from the location where the identity check is performed.
Registration Authority	A designated unit of employees at InfoNotary responsible for performing the activities of registration, identification, and identity verification of users of trust services.
Third Party	A natural or legal person who relies on remote video identification or a trust service.
Trust Service, pursuant to Regulation (EU) № 2024/1183	An electronic service, usually provided for remuneration, consisting of one or more of the elements listed in Article 3, point 16 of Regulation (EU) 2024/1183.
National Level Trust Service	In accordance with clause 5.5.1.3 (a) of ETSI TS 119 612 URI: http://uri.etsi.org/TrstSvc/Svctype/RA
InfoNotary SignZone SDK (Software Development Kit)	A package of specialized software components for installation/integration into third-party mobile applications to provide/use INFONOTARY's trust services.

ABBREVIATIONS

RA	Registration Authority
TSP	Trust service provider
RVI	Remote video identification
CP	Certificate Policy
CPS	Certification Practice Statement
ETSI	European Telecommunications Standards Institute
EU	European Union
ISO	International Standardization Organization
OID	Object Identifier
PKI	Public Key Infrastructure

2. OBLIGATIONS FOR PUBLICATION AND MAINTENANCE OF REGISTERS

In accordance with clauses 2.1.1 and 2.3 of the INFONOTARY document Certification Practice Statement for Qualified Certification Services.

3. REMOTE VIDEO IDENTIFICATION SERVICE

3.1. General Characteristics and Description

The nationally qualified Remote Video Identification Service provided by INFONOTARY is implemented as a process of remote verification of the identity of natural persons and the identification of legal entities, where the Applicant/User is physically remote from the location where the verification and confirmation of their personal participation in the process and identity takes place.

The verification is carried out by the Provider in several steps and is based on:

1. Data personally provided by the Applicant/User:

- a digital copy of an identity document (Bulgarian identity document – ID card), including photos of the front and back of the document taken during the Remote Video Identification (RVI) process;
- a video recording of the natural person performing additional actions assigned during the process (e.g., reading aloud a displayed alphanumeric code or other);
- mobile phone number;
- unique identifier of the mobile device used to perform the process.

2. Collected identity and/or identification data of the Applicant/User from national registers of the primary data administrators

The service provision process is initiated by a natural person (Applicant/User) through the InfoNotary SignZone mobile application or a mobile application integrated with the InfoNotary Mobile Software Development Kit (InfoNotary SDK) by INFONOTARY, by starting an online automated session to collect the information necessary to verify their identity. The user provides the data and information following the sequence and instructions given by the automated guidance received within InfoNotary SignZone.

Starting the Remote Video Identification Service process via the InfoNotary SignZone mobile application guarantees that the Applicant accepts the rules and conditions for the provision and use of the service related to:

- Use of the InfoNotary SignZone application;
- The process of identity verification and confirmation;
- Consent to the provision and processing of their personal data by the Provider.

Verification of the data provided by the User and its confirmation is carried out on three levels:

Level I – Processing of photos in the mobile application before transmission to the Registration Authority (RA) – automated extraction and verification of data from the MRZ (machine-readable zone) on the back of the ID card photo.

Level II – Processing of data by the Provider's internal RA system – automated verification

of photos and videos for correctness for further processing, including matching of facial features, sound, text, and others.

Level III – Processing of data by an authorized RA Operator of the Provider.

The provision, collection, processing, verification, and storage of all data involved in the remote video identification process are carried out by all participants in compliance with the rules and procedures set forth in this document, as well as the conditions specified in other internal documents of the Provider.

The final verification and confirmation of the data and their linking to the User are performed after the completion of the online data collection session, at a subsequent stage, and based on the results of the preliminary checks carried out at previous levels, personally by a qualified employee/operator of the Registration Authority.

If the verification of the User's identity and/or legal entity status is positive, the validated data are recorded in the Provider's client registry, and a unique client profile is created for the natural or legal person. The data used during the verification process—including the photos and videos provided by the User, data obtained from national registers of primary data administrators, and those generated by the Registration Authority—are stored by the Provider for a period depending on the use of the remote identification result, as follows:

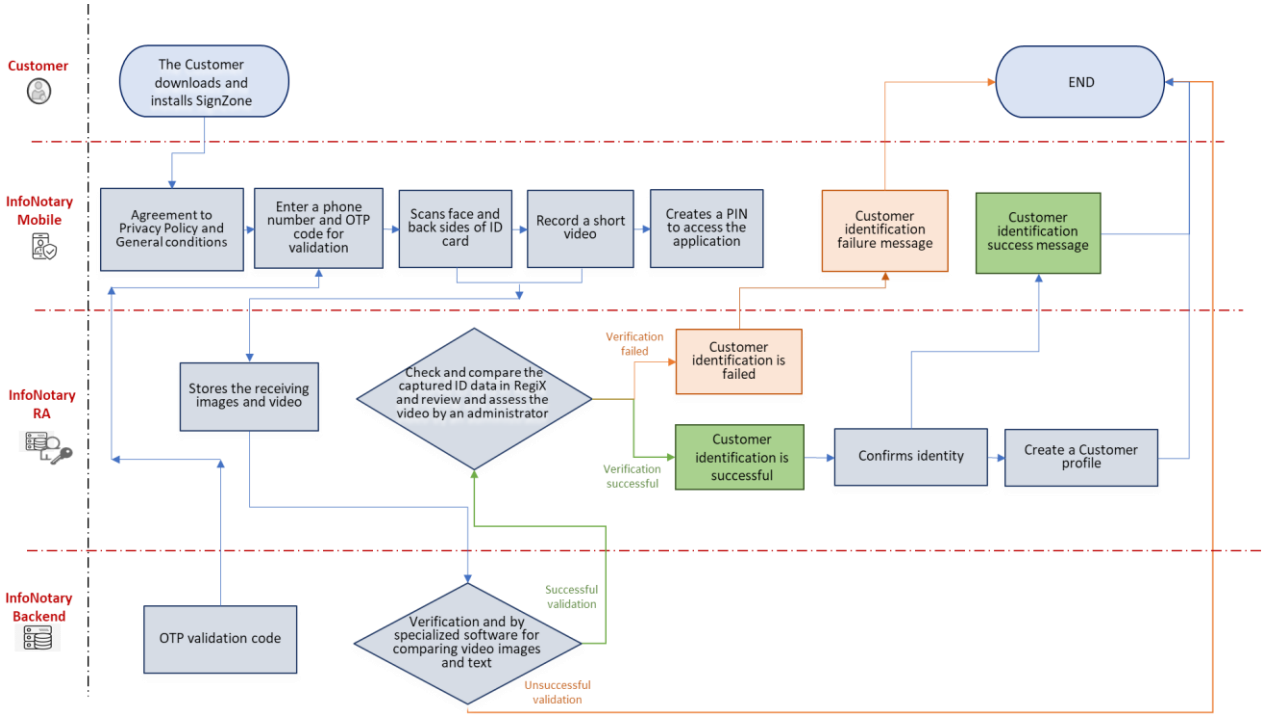
- For issuance and management of a qualified certificate for a qualified or advanced electronic signature or electronic seal – up to 10 years after the certificate's expiration;
- For issuance and management of an electronic identification means – up to 10 years after the validity of the means expires;
- For confirmation of the identity of a natural or legal person before a Third Party – for a period determined by the Third Party, but not longer than 10 years from the moment of confirmation.

Successful identification of the User enables them to subsequently request various certification services from the Provider or use services from Third Parties that have agreements with the Provider for this purpose.

If the verification result is negative (the provided data cannot be processed, lack necessary photos or audio recordings, facial characteristics do not match, there are discrepancies in the data or the user's civil status, or the operator has reasonable suspicion), the User is notified that the identification has failed. The data used in the verification process, which may include photos and videos provided by the User, data obtained from national registers of primary data administrators, and those generated by the Registering Authority, are deleted and not stored by the Provider.

The remote video identification process carried out by the Registering Authority ensures a security level equivalent to the physical presence of the user/applicant, in accordance with the normative requirements and European standards cited in section 1.1.

A schematic overview of the process is presented below:



3.2. PARTICIPANTS IN THE REMOTE VIDEO IDENTIFICATION SERVICE

3.2.1. Parties involved in the remote video identification process

The parties involved in the remote video identification process are:

- User/Applicant – A natural or legal person whose identity and/or legal status needs to be reliably verified and confirmed before registration and creation of a user profile in the Provider's systems for providing trust services or a third relying party;
- InfoNotary SignZone mobile application/InfoNotary Mobile SDK with remote video identification functionality – installed by the user on their smart device (smartphone or tablet) and used by them to initiate and carry out the onboarding process;
- Registration Authority (RA) of InfoNotary PLC – remotely performs the initial identification and confirmation of the Applicant's identity after verifying and confirming the results from the onboarding process performed by the Applicant;
- Certification Authority of InfoNotary PLC – a unit of the Provider responsible for issuing and managing qualified certificates;
- Third party – a legal entity, organization, administrative body, or local government authority, separate from the Provider, which relies on the trust services of InfoNotary PLC and uses, for its own purposes, the result of a Remote Video Identification Service used by its Applicant/User/Client.

3.2.2. User/Applicant

The Remote Video Identification Service may be used by Users who:

- Have downloaded and installed the InfoNotary SignZone mobile application / a third-party mobile application with integrated InfoNotary Mobile SDK on a smart device that

is solely under their control and for which the user has granted the application permission to access the device's camera and microphone;

- Have a mobile phone number under their control that can receive short text messages (SMS);
- Possess basic knowledge of using mobile applications and operating a built-in mobile device camera for capturing photos and videos;
- Have access to mobile internet with data transmission capabilities;
- Hold a valid Bulgarian identity document (ID card);
- Accept the terms of this document, the Provider's "Certification Practice Statement for Qualified Certification Services," the "General Terms of Use for Qualified Trust Services via Mobile Application," and the "Privacy Policy and Protection of Personal Data";
- Correctly follow the instructions for submitting the necessary data and documents for the purpose of remote video identification.

3.2.3. InfoNotary SignZone Mobile Application

The InfoNotary SignZone mobile application is a software solution specially developed by the Provider for the secure provision and use of trust services. The mobile application is also available in SDK format (InfoNotary Mobile SDK), allowing its functionalities to be integrated into third-party mobile applications. InfoNotary SignZone is available for download and use on mobile smart devices with Android and iOS operating systems.

The Remote Video Identification Service is part of the trust services provided by the Provider through the InfoNotary SignZone application. The mobile application ensures a reliable and controlled environment that guarantees the authenticity, integrity, and confidentiality of the electronic submission by the Applicant of a digital copy of their identity document and video session of their face.

The mobile application requires the Applicant to create a secret code (PIN) for accessing/logging into the application and for signing electronic documents using a cloud qualified electronic signature (Cloud QES).

The Applicant must not share the created PIN with third parties. From the moment the PIN is created, the Applicant is personally and solely responsible for keeping it secret and secure, as well as for all actions carried out by them or third parties using the PIN. Any use of the PIN is considered to be an action by the Applicant. The Provider is not responsible for the use of the PIN by the Applicant or for any unauthorized use of the PIN resulting from the Applicant's negligence.

If the Applicant enters the wrong PIN three (3) consecutive times for accessing the application or signing documents, their access or signing capabilities will be temporarily restricted. After the restriction period expires, they may try again.

The Applicant can change their PIN using the relevant functionality available in the "Settings" menu of the application.

If the User forgets or suspects the compromise of the PIN created during the initial registration, they can create a new PIN by undergoing the remote video identification process again. In this case, the certificates issued during the initial registration are terminated and is issued new ones to the Applicant.

3.2.4. Registration Authority

The Provider maintains Registration Authorities (RA), which collect, verify, and confirm identification data of individuals, legal entities, and organizations, as well as individuals representing legal entities (Applicant/User). The Registration Authority performs checks in accordance with the Provider's rules and procedures, fully complying with this "Policy and Practice for Provision of a Nationally Qualified Remote Video Identification" and other internal documents.

Регистриращите органи на Доставчика извършват дейности по първоначално идентифициране и потвърждаване на самоличността на лицата чрез:

The Provider's Registration Authorities carry out the initial identification and verification of persons through:

- Electronic verification of the Applicant identity (secured data exchange session) via information received from official primary registers maintained by central government administrations and executive agencies, accessible through the inter-register exchange platform (RegiX), to establish and confirm: **a)** the existence and civil status of the Applicant; **b)** ownership of the identity document; **c)** validity of the presented identity document; **d)** match between the Applicant and the photo on the submitted identity document, the photo received from RegiX, and the live video session;
- Verification of the identity of legal entities and organizations and the representative authority of individuals acting on behalf of legal entities via information received from RegiX or other sources and documents provided by the legal entity or a third party, to confirm the existence of the legal entity and the powers of the individual to represent it.

The Registration Authority collects and stores in digital form the data and documents used for verifying and confirming the identity and representation authority of the User.

It also gathers the required information for verifying the identity of the Applicant through their use of the InfoNotary SignZone mobile application (or the InfoNotary Mobile SDK) installed on their smart device. Additionally, for the purposes of the remote video identification process, the Registration Authority collects identification data related to the smart device on which the InfoNotary SignZone app is installed.

A check and validation of the mobile phone number under the Applicant's control is performed, confirmed by an OTP code sent via SMS.

Remote identification of legal entities and the representation authority of individuals representing them is conducted by verifying the current registered status of the legal entity in the Commercial Register. Additional sources of information and documents provided by the legal entity or a third party may also be used to confirm the representation authority of the individual.

The RA activities are performed by qualified personnel—operators who possess the necessary professional training, knowledge, skills, and experience, and who have completed appropriate training regarding security rules and personal data protection. Each operator accesses the Provider's internal RA system using a specially issued operator certificate and holds a qualified electronic signature, which is used to confirm the outcome of the remote identification check. All actions by operators related to processing User-provided data (photos and video), as well as data received from official primary registers via RegiX, are performed personally and strictly for the authorized activities and processing purposes defined by the Provider.

Operators process User data solely for the purpose of verifying the identity and/or legal status of individuals or legal entities, based on a specific request initiated by the Applicant through the remote video identification process.

The RA verifies the authenticity of the information using all legally permitted means.

The Provider reserves the right to modify the requirements for information and documents necessary for verifying the identity of individuals or legal entities if needed to comply with its trust service policies or legal obligations.

The Provider may delegate rights and authorize third parties to act as Registration Authorities on behalf of and at the expense of InfoNotary PLC. The Provider assigns RA activities based on a bilateral written agreement.

Authorized Registration Authorities perform their activities in accordance with this document, the Provider's "Certification Practice Statement for Qualified Certification Services," its trust service policies, and documented internal procedures and rules.

3.2.5. Certification Authority

The Certification Authority of InfoNotary is a unit within the Provider's infrastructure that is responsible for issuing and managing qualified certificates, using the result of the verification performed by the Registration Authority.

3.2.6. Third Party

A Third Party is a legal entity/organization separate from the Provider (e.g., another QTSP, financial institution, insurance company, etc.), administrative body, or local government authority that relies on InfoNotary's trust services and uses the result of the Remote Video Identification Service for its own purposes, provided to its Applicant/User/Client by the Provider.

The Third Party must sign an individual agreement with the Provider for using the Provider's RVIS for its clients, users, or employees. The Third Party must also complete an integration with the Provider's systems via API/SDK to request and receive the result of the RVIS process.

4. OPERATIONAL CONDITIONS AND PROCEDURES FOR PROVIDING THE REMOTE VIDEO IDENTIFICATION SERVICE

The operational activities related to the provision of the Remote Video Identification Service (RVIS) include ensuring access to download the InfoNotary SignZone, identification and confirmation of the User's identity, and creation of a client profile.

4.1. DOWNLOADING THE MOBILE APPLICATION - INFONOTARY SIGNZONE

The InfoNotary SignZone is published in the electronic stores App Store and Google Play. Depending on the operating system of the User's smart device, they can download and install it.

4.2. IDENTITY VERIFICATION OF A NATURAL PERSON THROUGH REMOTE VIDEO IDENTIFICATION

4.2.1. Establishing the identity of an individual through Remote Video Identification

4.2.1.1. Natural Person acting in Personal Capacity

The initial identification and verification of individuals' identity through remote video identification is initiated by the Users via the InfoNotary mobile application. The User should:

- Download and install the InfoNotary SignZone for the respective operating system;
- Possess a valid identity document;
- Accept the terms of this document, the Provider's Certification Practice Statement for Qualified Certification Services, the General Terms of Use of the application, and the Privacy and Data Protection Policy;
- Provide and follow the instructions for validating a mobile phone number under their control;
- Start the registration and remote identification process;
- Personally, and voluntarily capture and submit their identity document;
- Personally, and voluntarily capture and submit a video recording in which their face and eyes are clearly visible, while performing specified actions in a defined sequence, as instructed in the application;
- Explicitly consent to the collection of their personal data from the submitted identity document, as well as other specific data required for the provision of the Service;
- Create a secret code (PIN) for accessing the application.

During the initial identification and confirmation of the identity of individuals through remote video identification, the actual existence and civil status of the individual at the time of requesting/using the service are established.

The Registration Authority, via electronic means through RegiX, checks and confirms the identity of the data and circumstances gathered from the identity document submitted by the individual against those recorded in national registers, as follows:

- Personal, Patronymic and Family Name (in Cyrillic and Latin script);
- Date and place of birth;
- Nationality;
- Gender;
- Address, city, country, postal code;
- Unified Civil Number (UCN);
- ID document number: identity card or passport;
- Issuing authority, date of issuance and validity of the identification document as of the date of the Remote Video Identification (RVI) Service (the document must not be stolen, lost, revoked, or declared invalid on any other grounds);
- Actual existence and civil status of the individual.

The Registration Authority reviews the recorded video to verify the life status of the person, ownership of the presented identification document, and to ensure that the person in the video is the same as the one shown in the ID document.

After successful verification and confirmation of the User's identity, the Registration Authority creates a client profile in the Provider's systems. The User is notified via the mobile application that the identification has been successful.

If there is a discrepancy in the data or in the civil or life status of the individual, or if the operator suspects irregularities in any of the provided data or recorded materials (e.g. the integrity of the ID document, signs of coercion, or other suspicious circumstances), the identification of the person is rejected. The User is notified via the mobile application that the identification has failed, along with the reasons for the rejection. Once the issues have been resolved, the User may restart the process through InfoNotary SignZone.

The Registration Authority operator who conducted the verification confirms the successful or unsuccessful identification by signing, using a qualified electronic signature, a Report on the Verification and Confirmation of Identity of a Natural Person through Remote Video Identification.

The images and video recordings submitted by the User during the identification process are also reviewed by specialized software for video image and text comparison, which performs automated analysis of image quality, facial match between the photo on the ID document and the video, as well as other visual details.

4.2.1.2. Natural Person acting as a Legal Representative of a Legal Entity/Organization

In the case of remote video identification of natural persons who are legal representatives of legal entities, it is confirmed that, at the time of requesting/using the service, the legal entity exists and the natural person (Applicant/User) possesses the necessary representative authority.

To establish and confirm these circumstances, the steps described in section 4.2.1.1. are followed, and in addition, the User must provide:

- the name and legal form of the legal entity/organization;
- UIC/BULSTAT number.

In this case, in addition to the identification checks for the natural person described in section 4.2.1.1., the Registration Authority also verifies and confirms (via RegiX) the current registered status of the legal entity in the Commercial Register, including:

- name of the legal entity;
- •legal form;
- •UIC/BULSTAT number;
- names of the official representatives;
- address, city, country, postal code;
- operational status.

Additionally, the User must submit documents proving their representative authority on behalf of the legal entity—e.g. a court decision, certificate of good standing, notarized power of attorney, or other empowering document. These documents are submitted via the InfoNotary

SignZone mobile application.

The Registration Authority electronically verifies and confirms the identity of the data and circumstances provided by the User with those found in national registers via RegiX, and also checks and confirms any additional documents through other sources or third parties.

After successful verification and confirmation of both the User's identity and the legal entity's status, the Registration Authority creates a client profile in the Provider's systems. The User is notified in the mobile application that the identification was successful.

If there is a discrepancy in the data of the natural or legal person, in the representative authority of the individual with respect to the legal entity, or in the civil or life status of the individual, or if the operator suspects inconsistencies in any of the provided data or elements in the captured images and video, the identification is rejected. The User is notified via the mobile application that the identification was unsuccessful, along with the reasons for the rejection. Once the causes of the unsuccessful identification are resolved, the User may initiate the process again via InfoNotary SignZone.

The Registration Authority operator who conducted the verification confirms the successful or unsuccessful identification of the User by signing, with a qualified electronic signature, a Report on the Verification and Confirmation of the Identity of a Natural Person through Remote Video Identification.

5. CONTROL OF EQUIPMENT, PROCEDURES AND MANAGEMENT

The Remote Video Identification Service is carried out by the Registration Authority, which is a functional part of the Provider's established and audited PKI infrastructure, in compliance with the applicable regulatory requirements. This infrastructure is used for the provision of qualified trust services. In this context, the management and operational control of equipment, security, and its activities are governed by the rules and procedures described in the " Certification Practice Statement for Qualified Certification Services" document of InfoNotary. Where applicable, the present document supplements those rules and procedures, taking into account the specific functionality of the service, the automated procedures for the collection of personal data, their verification, and the confirmation of the Applicant's identity.

5.1. Physical Control

In accordance with section 5.1 of InfoNotary's Certification Practice Statement for Qualified Certification Services.

5.1.1. Premises Location and Construction

In accordance with section 5.1.1 of InfoNotary's Certification Practice Statement for Qualified Certification Services.

The Registration Authority uses dedicated office premises to which only authorized personnel (operators and system administrators) have access. These individuals are responsible for processing and storing the data collected during the remote video identification process..

5.2. PHYSICAL ACCSESS

In accordance with section 5.1.2 of InfoNotary's Certification Practice Statement for Qualified Certification Services.

5.2.1. Power supply and climatic conditions

In accordance with section 5.1.3 of InfoNotary's Certification Practice Statement for Qualified Certification Services.

5.2.2. Flooding

In accordance with section 5.1.4 of the INFONOTARY document Certification practice statement for qualified certification services

5.2.3. Fire alarm and protection

In accordance with section 5.1.5 of the INFONOTARY document Certification practice statement for qualified certification services

5.2.4. Data storage

In accordance with section 5.1.6 of the INFONOTARY document Certification practice statement for qualified certification services

5.2.5. Decommissioning of technical components

In accordance with section 5.1.7 of the INFONOTARY document Certification practice statement for qualified certification services.

5.2.6. Duplication of components

In accordance with section 5.1.8 of the INFONOTARY document Certification practice statement for qualified certification services.

5.3. PROCEDURAL CONTROL ПРОЦЕДУРЕН КОНТРОЛ

In accordance with section 5.2 of the INFONOTARY document Certification practice statement for qualified certification services.

5.3.1. Positions and functions

In accordance with section 5.2.1 of the INFONOTARY document Certification practice statement for qualified certification services.

5.3.2. Number of personnel per task

In accordance with section 5.2.2 of the INFONOTARY document Certification practice statement for qualified certification services.

5.3.3. Identification and authentication for each position

In accordance with section 5.2.3 of the INFONOTARY document Certification practice statement for qualified certification services.

5.3.4. Requirements for separation of duties for different functions

In accordance with section 5.2.4 of the INFONOTARY document Certification practice statement for qualified certification services.

5.4. PERSONNEL CONTROL, QUALIFICATION, AND TRAINING

In accordance with section 5.3 of InfoNotary's Certification Practice Statement for Qualified Certification Services.

Additionally, InfoNotary personnel performing the functions of operators within the

Registration Authority possess the necessary professional training and experience to reliably identify Users, adhering to approved internal operational requirements and procedures. RA operators undergo periodic additional training in line with current requirements in the field of trust services, including training on the software and equipment in use, training on the verification of documents and their security features, as well as in cases of changes in national legislation or modifications to the Provider's documentation and operational practices.

5.4.1. Requirements for independent suppliers

In accordance with section 5.3.1 of the INFONOTARY document Certification practice statement for qualified certification services.

Documentation provided to employees

In accordance with section 5.3.2 of the INFONOTARY document Certification practice statement for qualified certification services.

5.5. PROCEDURES FOR CREATING AND MAINTAINING LOGS OF INSPECTIONS

In accordance with section 5.4 of the INFONOTARY document Certification practice statement for qualified certification services

5.5.1. Frequency of record creation

In accordance with section 5.4.1 of the INFONOTARY document Certification practice statement for qualified certification services.

5.5.2. Retention period of records

In accordance with section 5.4.2 of the INFONOTARY document Certification practice statement for qualified certification services".

5.5.3. Protection of records

In accordance with section 5.4.3 of the INFONOTARY document Certification practice statement for qualified certification services.

5.5.4. Procedure for creating backups of records

In accordance with section 5.4.4 of the INFONOTARY document Certification practice statement for qualified certification services.

5.6.ARCHIVE

In accordance with section 5.5 of InfoNotary's Certification Practice Statement for Qualified Certification Services.

In addition, the Provider maintains an internal archive of the evidence from the process of proving the identity and authenticity of the Users in a manner that prevents falsification and alteration; ensures the confidentiality of the information; and provides the capability for searching, retrieving, and re-verifying the identity verification results.

5.6.1. Types of archives

In accordance with section 5.5.1 of the INFONOTARY document Certification practice statement for qualified certification services.

5.6.2. Retention period

In accordance with section 5.5.2 of the INFONOTARY document Certification practice statement for qualified certification services.

5.6.3. Archive protection

In accordance with section 5.5.3 of the INFONOTARY document Certification practice statement for qualified certification services.

5.6.4. Archive recovery procedures

In accordance with section 5.5.4 of the INFONOTARY document Certification practice statement for qualified certification services.

5.6.5. Requirements for date and time stamping of records

In accordance with section 5.5.5 of the INFONOTARY document Certification practice statement for qualified certification services.

5.6.6. Archive storage

In accordance with section 5.5.6 of the INFONOTARY document Certification practice statement for qualified certification services.

5.6.7. Procedures for obtaining and verifying archive information

In accordance with section 5.5.7 of the INFONOTARY document Certification practice statement for qualified certification services.

5.7. ACTION IN THE EVENT OF DISASTERS AND ACCIDENTS AND INCIDENTS RELATED TO DAMAGES IN HARDWARE, SOFTWARE AND / OR DATA

In accordance with section 5.7.1 and section 5.7.2 of the INFONOTARY document Certification practice statement for qualified certification services

5.8. PROCEDURES FOR TERMINATION OF PROVIDER'S ACTIVITIES

5.8.1. Termination of activities

In accordance with section 5.8.1 of the INFONOTARY document Certification practice statement for qualified certification services.

5.8.2. Transfer of activities to another qualified provider of qualified certification services

In accordance with section 5.8.2 of the INFONOTARY document Certification practice statement for qualified certification services.

5.8.3. Revocation of the Provider's qualified status

In accordance with section 5.8.3 of the INFONOTARY document Certification practice statement for qualified certification services.

6. TECHNICAL AND COMPUTER SECURITY CONTROL

In accordance with sections 6.4 and 6.5 of the INFONOTARY document Certification practice statement for qualified certification services

7. MONITORING AND CONTROL OF ACTIVITIES

In accordance with section 8 of the INFONOTARY document Certification practice statement for qualified certification services.

7.1. Regular or extraordinary audit

In accordance with section 8.1 of the INFONOTARY document Certification practice statement for qualified certification services.

7.2. Qualification of Auditors

In accordance with section 8.2 of the INFONOTARY document Certification practice statement for qualified certification services.

7.3. Relationship between auditors and the organization being audited

In accordance with section 8.3 of the INFONOTARY document Certification practice statement for qualified certification services.

7.4. Scope of the audit

In accordance with section 8.4 of the INFONOTARY document Certification practice statement for qualified certification services.

7.5. Taking actions to correct deficiencies

In accordance with section 8.5 of the INFONOTARY document Certification practice statement for qualified certification services.

7.6. Reporting of results

In accordance with section 8.5 of the INFONOTARY document Certification practice statement for qualified certification services.

8. OTHER BUSINESS AND LEGAL TERMS

8.1. PRICES AND FEES

In accordance with section 9.1 of the INFONOTARY document Certification practice statement for qualified certification services.

8.1.1. Remuneration under the Contract for Qualified Certification Services

In accordance with section 9.1.1 of the INFONOTARY document Certification practice statement for qualified certification services.

8.1.2. Invoicing

In accordance with section 9.1.2 of the INFONOTARY document Certification practice statement for qualified certification services.

8.1.3. Policy for Certificate Return and Refund

In accordance with section 9.1.3 of the INFONOTARY document Certification practice statement for qualified certification services.

8.2. FINANCIAL RESPONSIBILITIES

8.2.1. Financial Responsibilities

In accordance with section 9.2.1 of the INFONOTARY document Certification practice statement for qualified certification services.

InfoNotary shall be liable for the provision of the Remote Video Identification Service to all third parties who rely on the completed identification, as well as to the individual or legal entity for any damages caused due to failures in verifying the identity/authenticity of the person. InfoNotary bears such liability only in the absence of circumstances that exclude the Provider's responsibility.

8.2.2. Insurance of Activity

In accordance with section 9.2.2 of the INFONOTARY document Certification practice statement for qualified certification services.

8.2.3. Insurance Coverage for End Users

In accordance with section 9.2.3 of the INFONOTARY document Certification practice statement for qualified certification services.

- The insurance does not cover, and the Provider is not liable for damages resulting from:
- Non-compliance by the Users of the Remote Video Identification Service with their obligations arising from the terms of this document, the Provider’s Practice for the Provision of Qualified Trust Services, and the General Terms and Conditions for using qualified trust services via the mobile application;
- Loss of the mobile device or compromise of the secret code (PIN) for accessing the application by the User, due to failure to exercise due care in protecting or using it;
- Malicious actions by third parties (hacking attacks, theft of the mobile device, access to identification methods, etc.);
- Illegal actions by the User, relying parties, and third parties;
- Force majeure, accidents, and other events beyond the Provider’s control.

8.3. CONFIDENTIALITY OF INFORMATION

In accordance with section 9.3 of the INFONOTARY document Certification practice statement for qualified certification services.

8.3.1. Scope of Confidential Information

In accordance with section 9.3.1 of the INFONOTARY document Certification practice statement for qualified certification services.

Additionally, the Provider considers confidential the information contained in and relating to:

- Any information about the Applicant/User/Client of the Provider’s Remote Video Identification Service, other than that contained in the result of the Remote Video Identification (RVIS);
- The reason for the confirmation or refusal to perform the service, other than the information about the status.

8.3.2. Information outside the scope of confidential information

In accordance with section 9.3.2 of the INFONOTARY document Certification practice statement for qualified certification services.

8.3.3. Obligation to Protect Confidential Information

In accordance with section 9.3.3 of the INFONOTARY document Certification practice statement for qualified certification services

The Registration Authorities, the Applicant/User/Client of the Provider's Remote Video Identification Service, or their authorized representatives, are not entitled to disclose or allow the disclosure of information that became known to them during or in connection with the performance of their obligations under contracts with the Provider, without prior explicit written permission from the other party.

8.4. CONFIDENTIALITY OF PERSONAL DATA

In accordance with section 9.4 of the INFONOTARY document Certification practice statement for qualified certification services

8.5. NTELLECTUAL PROPERTY RIGHTS

In accordance with section 9.5 of the INFONOTARY document Certification practice statement for qualified certification services.

8.6. OBLIGATIONS, LIABILITY AND WARRANTIES

In accordance with section 9.6 of the INFONOTARY document Certification practice statement for qualified certification services.

When providing the Remote Video Identification Service, the Provider guarantees the correct identification of persons at the time of providing the service.

8.6.1. Obligations and Responsibilities of Users

In accordance with section 9.6.1 of the INFONOTARY document Certification practice statement for qualified certification services

Additionally, Users of the Remote Video Identification Service have the following obligations and responsibilities:

- To comply with the terms of this document, the Provider's Practice for the Provision of Qualified Trust Services, the General Terms of Use of the mobile application, and the Privacy and Personal Data Protection Policy;
- To provide truthful, accurate, and complete information as required by the Provider, in accordance with regulatory requirements and applicable Policies and Practices;
- Not to make false statements or submit false documents to the Registration Authority relevant to the provision of the service;
- To strictly adhere to the security requirements set by the Provider;
- To keep the created secret code (PIN code) for accessing the application confidential and prevent its disclosure or unauthorized use.

Users are liable to InfoNotary in all cases of failure to fulfill the obligations specified in this

document, the Provider's Practice for the Provision of Qualified Trust Services, and the General Terms of Use of the application, whereby the Provider may hold the User responsible for damages.

8.6.2. Guarantees and liability of the Registration Authority

In accordance with section 9.6.2 of the INFONOTARY document Certification practice statement for qualified certification services.

8.6.3. Obligations and Responsibilities of Third Parties

The obligations, responsibilities, and manner of integration of Third Parties with the Provider's systems are regulated by the individual contract concluded with the Provider.

8.7. DISCLAIMER OF LIABILITY

In accordance with section 9.7 of the INFONOTARY document Certification practice statement for qualified certification services.

Additionally, InfoNotary is not liable for damages caused by:

- Failure to comply with the obligations of the Users of the Remote Video Identification Service and Third Parties arising from the terms of this document, the Provider's Practice for the Provision of Qualified Trust Services, and the General Terms of Use of qualified trust services through the mobile application;
- Loss of a mobile device or compromise of the created secret code (PIN code) for accessing the application by the User due to failure to exercise due care in its protection or use;
- Malicious actions by third parties (hacking attacks, theft of mobile devices, unauthorized access to identification methods, etc.);
- Illegal actions by Users and Third Parties;
- Force majeure, accidents, and other events beyond the Provider's control.

The Provider is not liable for damages suffered by a Third Party resulting from the Third Party's failure to fulfill its obligations and failure to exercise due care as stipulated in the concluded contract and this document.

8.8. ОГРАНИЧЕНИЕ НА ОТГОВОРНОСТТА

In accordance with section 9.8 of the INFONOTARY document Certification practice statement for qualified certification services.

8.9. COMPENSATION TO THE PROVIDER

In all cases of non-fulfillment of obligations by the Users of the Remote Video Identification Service and Third Parties arising from the terms of this document, the Provider's Practice for the Provision of Qualified Trust Services, and the General Terms of Use for qualified trust services via the mobile application, the Provider will hold the Users of the Remote Video Identification Service and Third Parties liable for damages.

8.10. TERM AND TERMINATION

8.10.1. Term

This "Policy and Practice for The Provision of A Nationally Qualified Remote Video Identification Service" enters into force from the moment of its approval by the Board of Directors of Infonotary PLC and its publication at: http://www.infonotary.com .

This document is valid until it is changed or its invalidity is published in the Document Register and on the Provider's internet portal.

8.10.2. Termination

This "Policy and Practice for The Provision of a Nationally Qualified Remote Video Identification Service" ceases to be effective upon termination of the Provider's activity..

8.10.3. Effect of termination

After termination of its effect for users, the provisions regarding the Provider's obligations to maintain an archive of documents and information, in the scope and period described in this document, remain in force.

8.11. INDIVIDUAL NOTIFICATION AND COMMUNICATION BETWEEN PARTICIPANTS

In accordance with section 9.11 of the INFONOTARY document Certification practice statement for qualified certification services.

8.12. AMENDMENTS

This "Policy and Practice for The Provision of a Nationally Qualified Remote Video Identification Service" may be amended at any time, with each amendment coming into effect after approval by the Board of Directors of Infonotary EAD and being publicly accessible to all interested parties at https://www.infonotary.com .

Any person may submit proposals for changes (structural and substantive) and notes on detected errors to the contact email and postal addresses indicated in this document.

8.13. DISPUTE RESOLUTION AND JURISDICTION

In accordance with section 9.13 of the INFONOTARY document Certification practice statement for qualified certification services.

8.14. APPLICABLE LAW

In accordance with section 9.13 of the INFONOTARY document Certification practice statement for qualified certification services.

8.15. COMPLIANCE WITH APPLICABLE LAW

This "Policy and Practice for The Provision of a Nationally Qualified Remote Video Identification Service" is developed in accordance with the requirements of Regulation (EU) 910/2014 (amendment with Regulation 2024/1183) and national legislation.

8.16. OTHER PROVISIONS

This document contains no other provisions.