PRIVACY POLICY AND PROTECTION OF PERSONAL DATA

OF

QUALIFIED TRUST SERVICE PROVIDER

INFONOTARY PLC

VERSION 1.2

Entry into force 16.12.2024 г.

TABLE OF CONTENTS

I. INTRODUCTION

The PRIVACY POLICY AND PROTECTION OF PERSONAL DATA of "INFONOTARI" PLC ("Policy/Privacy Policy") is based on the requirements lay down in 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, and repealing Directive 95/46/EC (Regulation (EU) 2016/679) and Personal Data Protection Act.

All amendments of the Privacy Declaration shall be applied after its publication on INFONOTARY PLC's website.

All amendments and additions to the Privacy Policy will be applied after the publication of its current content, accessible through our website: http://www.infonotary.com

Data about the controller

INFONOTARY PLC (INFONOTARY/Provider) with UIC 131276827 registered office and headquarters at 16 Ivan Vazov St., 1000 Sofia, Bulgaria is a data controller, processing your personal data by lawful, fair and transparent manner and in compliance with the provisions set in Personal Data Protection Act and Regulation (EU) 2016/679.

You may contact us at the registered office: 16, Ivan Vazov St, 1000 Sofia, Bulgaria,

phone: +359 2 921 08 90, 02 451 08 90

The Data Protection Officer of INFONOTARY PLC is:

Emil Kirov

address: 16, Ivan Vazov St, 1000 Sofia, Bulgaria

phone: +359 2 921 08 90

email address: dpo@infonotary.com

Terms and abbreviations

1. „Controller" means any natural or legal person, in this case INFONOTARY, who determines the purposes and means of processing personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

2. „Personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number,

location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

3. „Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

4. „Pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

5. „Data subject" means a natural person who, in a personal capacity or as legal or authorized representatives of a natural or legal person, apply for and/or use the trust services of "INFONOTARY" PLC and whose data is processed in connection with the provision of trust services and the conclusion of a contract (referred to as short "customer"/"you");

6. „Consent of the data subject" means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

7. „Applicable legislation and regulations" means the regulations of the European Union, including but not limited to the General Data Protection Regulation EU 2016 / 679, the Personal Data Protection Act, the Electronic Document and Electronic Trust Services Act, as well as any other applicable legal act regarding personal data.

II. PERSONAL DATA WHICH ARE BEING PROCESSED

INFONOTARY PLC (INFONOTARY) is a qualified trust service provider, providing qualified trust services in accordance with REGULATION (EU) No 910/2014 and national law, recognized by the Bulgarian Supervisory Authority.

When processing personal data, INFONOTARY complies with all applicable personal data protection regulations, including Regulation (EU) 2016/679.

Depending on the specific objectives and grounds INFONOTARY processes the personal data indicated below separately or in combination, as follows:

1. Personal data provided by you, that is necessary for identification and confirmation of identity when providing the trusted services as well as fulfilment of the contractual obligations between INFONOTARY and the Customer:

1.1. Physical presence at the office of the Registration Authority of Infonotary:

- Names (according to an identity document), personal identification number or personal number of a foreigner, date of birth for a foreigner, nationality, address, phone number, e-mail;
- Names, personal identification number, address and other data of your representative, specified in the document whereby you authorized him/her to represent you before INFONOTARY;
- Identity document number, date of issue, date of expiry and issuing authority;
- Data retrieved from national registers of primary data administrators, when performing an automated official verification of identity document validity and vital status and/or automatically downloaded data from the machine-readable part of the identity document;
- Data collected upon payment – number of credit or debit card, bank account and other payment information collected upon processing the payments made by you.

1.2. When using the Provider's mobile application SignZone - or the INFONOTARY's SDK integrated into a third-party mobile application:

- Names (by identity document), personal identification number; number, date of issue and validity of identity document; issuer of identity document; gender; date of birth; nationality; address; phone number; e-mail;
- Biometric data: a) electronic copy (photos) of an identity document along with all automatically downloaded data from its machine-readable part; b) video recording of the person, along with a recording of the text/code spoken by him; (c) a photo of the person retrieved from the national registers of primary data administrators;
- Data retrieved from national registers of primary data administrators, when performing an automated official verification of identity document validity and vital status;
- Data retrieved from national registers of primary data administrators when performing an electronic identification service initiated by you or a relying party.
- Report of verification and confirmation of the identity of a natural person through remote video identification with results of the presence or absence of a match between the scanned identity document, the data from the official registers and the video recording;

- Data used for addressing of electronic documents that are sent by you or to you for signing via SignZone, (ID number, telephone number, e-mail address);
- Data collected when authenticating to systems and applications;
- Data collected during payment – bank account number and other payment information, in connection with payments made by you for services provided.

Usage of the SignZone application requires from the customer to go through a registration process and remote video identification. The customer, before starting the remote video identification process, it is necessary to give his/her explicit consent to be identified and the voluntarily provided by him/her personal data (including biometrics) to be processed in the manner mentioned below in order to use trusted services through the application. The customer confirms that he has accepted the terms of this Policy by completing/checking the electronic registration form in the mobile application. Placing the sign and continuing the registration process is considered as an electronic statement within the meaning of the Electronic Document and Electronic Trust Services Act and unambiguously indicates acceptance and compliance with the requirements in this Policy.

During the remote video identification, INFONOTARY carries out semi-automated processing (through an operator) of those specified in item 1.2. data and makes a decision based solely on this method of processing, which gives rise to the following legal consequences for the client - confirmation of identity, conclusion of a contract for the use of authentication services, issuance of a qualified certificate for a cloud-based qualified electronic signature and a means of electronic identification, as well as providing access to INFONOTARY's qualified trusted services available through SignZone.

If the customer wish to use the INFONOTARY's services, but do not wish his/her personal data (including biometric data) to be processed in the above-described manner or to be the subject of a decision based solely on semi-automated processing, the customer can go through identification at an office of the PROVIDER's Registration Authority and request a trusted services that do not require the use of a mobile application.

Depending on the functionalities supported by the device on which SignZone is installed, the customer may use biometric data (fingerprint, facial recognition, etc.) to log into the application instead of the personal identification code created by him. When using this functionality, the customer's biometric data remains solely within the device and the application installed on it and is under the control of the customer at all times. This data is not processed and stored by the PROVIDER.

1.3. Data provided when participating in games, lotteries and/or other seasonal or promotional campaigns organized by INFONOTARY and addressed to an unlimited number of persons, including through social networks;

1.4. INFONOTARY may receive data about the applications, browsers, and the type of device used from the customer to access the PROVIDER's website or other Internet and mobile applications. This information may include device ID, application version number, operating system version, mobile network information including carrier name and phone number, IP address.

2. Other data in the process of providing services by INFONOTARY:

- Video recording of a visit to the central office of INFONOTARY, prepared with video surveillance equipment for security purposes and for ensuring safety service to employees and customers;
- Records of calls made to and from the INFONOTARY contact centre, e-mails, letters, complaints, requests, complaints and other feedback we receive from customers.
- Video recording or photography, made in accordance with the previously announced conditions for participation in games, lotteries and/or other promotional campaigns, organized by INFONOTARY and addressed to an unlimited number of persons, including through social networks.

In case of refusal to voluntarily provide required personal data, the PROVIDER will not be able to provide you with its products and services.

III. OBJECTIVES AND LEGAL GROUNDS FOR THE PROCESSING OF PERSONAL DATA:

INFONOTARY processes your data on the basis of Art. 6, paragraph 1, letters "a", "b", "c" and "e" of EU Regulation 2016/679 and for the following purposes:

1. To perform all activities as a Trust Service Provider and to manage its relationships with customers:

- Obtaining preliminary information necessary to conclude a contract for services;
- Identification and confirmation of a customer identity, who are using trusted services providing by INFONOTARY; fulfilment of requests for provisioning of information and clarification of the services that are being currently used.
- Updating your personal data provided upon registration/signing a contract for services and products provided by INFONOTARY, as well as for the duration of your contractual relationship with INFONOTARY.
- Verification the type of services registered and used by you, at your request;

- Complaint/objection or to protect our customers and INFONOTARY from fraud and abuse by third parties. Providing of information about services that are being currently used;
- Consideration of received objections, complaints, carrying out control, providing feedback;
- Technical assistance and support provided by phone, email or in place regarding the use of INFONOTARY's trusted services;
- Settling disputes before the competent authorities (court, arbitration, conciliation commission, administrative bodies, etc.) relating the INFONOTARY's activities.

2. To meet the legal obligations related to the provision of trust services as a Qualified Trust Service Provider under Regulation (EU) No 910/2014 and Electronic Document and Electronic Trusted Services Act, tax and accounting legislation and other applicable legislation relevant to the INFONOTARY's activities.

3. Where your explicit consent is required for the processing of relevant personal data and you have provided this consent for their processing. In cases where such consent is required to process your personal data and you make an informed decision not to provide it, INFONOTARY may not be able to provide the relevant product/service for which consent was required.

4. INFONOTARY processes the respective data provided with the customer's consent for their processing to include your name, photos, video and other forms of presence in advertising and media publications of INFONOTARY as a result of your participation in lotteries and games, or such of our partners and/or the social networks.

When processing personal data for a particular purpose is based on your consent, you may withdraw it at any time without prejudice to the legality of the processing prior to its withdrawal.

5. INFONOTARY processes your data for the following legitimate interests:

- Preparing and keeping statistical information and aggregate data - INFONOTARY
- Performs the analysis to develop and improve the services provided and the customer service;
- When providing data to third parties: when performing legal or contractual obligations of INFONOTARY or on other valid legal grounds.

IV. CATEGORIES OF THIRD PARTIES - RECIPIENTS OF PERSONAL DATA

In compliance with the requirements of Regulation (EU) 2016/679 INFONOTARY has the right to disclose personal data, they process to the following categories of recipients:

- Natural persons to whom the data refer;
- Third parties, natural persons, legal entities, public authorities and institutions, external and internal auditors, insurance companies, supervisory and regulatory authorities, when performing legal or contractual obligations of INFONOTARY or on other valid legal grounds, for instance, detecting, preventing or performing other activities regarding fraud, technical or security-related problems.
- State and government institutions when it is legally and explicitly required.
- Persons assigned by INFONOTARY to support equipment and software used for processing your personal data;
- Security companies licensed to carry out private security activity which are processing video recordings from offices of INFONOTARY in the process of controlling the access to these places;
- Companies providing services related to the organization, safekeeping, indexing and erasure or destruction of archives stored electronically and/or in paper;
- Persons who process personal data on behalf of INFONOTARY (Processors), such as the INFONOTARY's Registration Authorities. Processors perform their tasks in compliance with a contract or another legal document and according to the instructions of INFONOTARY.
- Processors provides sufficient guarantees to implement appropriate technical and organizational measures that the processing will meet the requirements of Regulation (EU) 2016/679.

Transfers of personal data to a third country or international organization

INFONOTARY will comply with the requirements of Regulation (EU) 2016/679 in case there is a need to transfers of personal data to a third country or an international organization, including the possible subsequent transfer of personal data from a third country or international organization to another country or organization.

V. PERIOD FOR STORAGE OF PERSONAL DATA

The period of storage of your personal data depends on the processing purposes for which they were collected. INFONOTARY processes your personal data for the terms established in the legislation in force in the country. Personal data for which there is no express

legal storage obligation will be deleted after the purposes for which they were collected and processed have been achieved.

INFONOTARY, in accordance with its internal rules and procedures and the applicable legislation, processes and stores your PERSONAL data and information about you in the following terms:

Data types	Period for storage
Personal data collected, processed and archived for the purposes of providing trusted services, including through SignZone	For the entire period of provision of the relevant service and for a period of 10 (ten) years after termination of the use of the service.
Personal data collected, processed and archived for the purposes of providing an electronic identification service, including through SignZone	For the entire period of provision of the service and for a period of 10 (ten) years after its termination.
Personal data collected, processed and archived in the process of remote video identification - in case of a positive result of the identification (successful identification)	For the entire period of use of the relevant service, for the provision of which the remote video identification was performed and for a period of 10 (ten) years after termination of use of the service.
Documents sent for signing or signed via SignZone	All documents are stored in encrypted form for 12 months period from the date of their creation/signing or in a period agreed between the customer and the Provider.
Addressing data for electronic documents	All data used for the addressing of electronic documents (identification number, telephone number, e-mail address) are stored for a period of 10 (ten) years from the date of their creation
Personal data collected, processed and archived in the process of remote video identification - in case of a negative result of the identification (unsuccessful identification)	All collected customer data is deleted and/or pseudonymised in the PROVIDER's systems. The pseudonymised data is stored for a period of 10 (ten) years, starting from the date of the remote video identification.
Financial and accounting documents; invoices and other information related to tax and accounting legislation	Up to 10 (ten) years, starting from the beginning of the year following the one in which the payment was made.
System logs related to ensuring the reliable functioning of the services and the mobile application, for login a user profile, for authentication to systems and applications, for establishing technical problems, for technical support, for security protection, detection and prevention of: unauthorized attempts to access to users profiles and other malicious acts, and etc. The system logs may contain account/system/application login date and time, status, whether login was through	Up to 10 (ten) years from the generation of the relevant log.

a mobile app or desktop browser, IP address, URL, browser and device version information, and etc.	
Data processed on the basis of your explicit consent.	From the moment consent is given until it is withdrawn by the data subject.
Recording of phone calls.	Up to 2 (two) years from the conversation was made
Picture (Video recording) during a visit to NFONOTARY's own offices.	Up to 1 (one) year from the date of creation of the record.

INFONOTARI may store some of your personal data for a longer period until the expiration of the relevant limitation period for the purpose of protection: in case of customers's claims about the services provisioning/termination of registration/service contract and ets, as well as for a longer period, until the final settlement of an arising litigation, relating the above mentioned, with an effective court decision.

INFONOTARY's security measures for personal data protection

The personal data protection of customers is one of the main priorities of INFONOTARY.

The company updates continuously the technical and organizational measures applied, which are necessary to ensure a high level of security and data protection. In carrying out its activity INFONOTARY applies the quality management system certified according to ISO / IEC 9001: 2008 and ISO / IEC 27001: 2013 certified security management information system.

VI. CUSTOMERS RIGHTS REGARDING PERSONAL DATA PROCESSING BY INFONOTARY

As a customer and in relation to your personal data, you have the following rights:

1. To receive information about your personal data processed by INFONOTARY regarding a trusted services you use, by submitting a filled standard request form and identifying yourself with an identity document, at the INFONOTARY's central office and at the INFONOTARY's Registration Authorities offices. You can see an up-to-date list of offices at http://www.infonotary.com.

2. To request correction of your personal data when it is inaccurate or should be supplemented for processing purposes.

3. To request to erasure of your personal data be deleted - only in a following cases:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- The data subject withdraws consent on which the processing is based when the processing is based only of the explicit consent of the subject;

- There is no legal or contractual basis for their processing;
- The personal data have been unlawfully processed;
- The national or European legislation requires this.

4. To request that your personal data processing should be limited in any of the following cases:

- the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- observing the data subject rights lay down in Regulation (EC) 2016/679.

5. To request the portability of your personal data, relating to you and submitted to INFONOTARY, according to the data subject's rights pursuant in Regulation (EC) 2016/679 and if you comply with the INFONOTARY terms and conditions. Your right to data portability concerns personal data that comply with the following conditions:

- the processing is based on your explicit consent or a contractual ground;
- the processing is carried out by automated means.

All admissible request will be performed in a reasonable time, but no longer than one month from the receiving date.

6. To make an objection before INFONOTARY at any time, on grounds relating to your situation, for the processing of your personal data, which INFONOTARY is processing on a legitimate ground.

In case of objection to the processing of your personal data for other purposes, NFONOTARY will reply in a reasonable time, but no longer than one month, whether NFONOTARY considers your objection justified and whether shall terminate processing this personal data for such purposes.

7. To withdraw your consent for the processing of your personal data when the processing is based on your explicit consent.

8. To lodge a complaint with the Data Protection Commission if you consider that your rights regarding the processing of your personal data have been violated.

Submission of request

INFONOTARY provides the following possibilities for request submission as per Regulation (EU) 2016/679:

- A request submission form in paper – it should be filed at the INFONOTARY's central office and in the local offices of INFONOTARY's Registration authority. The list of these offices can be found here https://www.infonotary.com/.
- Electronic request submission form – it should be signed with a qualified electronic signature and sent to the following email address: dpo@infonotary.com .
- In order to get a correct reply from INFONOTARY, you should be duly identified, therefore in the request form, it is necessary to provide certain obligatory data:
- from your ID card/passport - ID card/passport number, expiry date, current address and ets.,
- phone number, e-mail as well as in what role would you like to exercise your rights under Regulation (EU) 2016/679 – for instance: client/former client, legal representative, actual owner, etc.

If the information provided is incorrect and/or incomplete, we may not be able to meet your request or part thereof.

Right to lodge a complaint with a supervisory authority

You have the right to lodge a complaint with the relevant supervisory authority, which in Bulgaria is the Commission for Personal Data Protection.

The Commission contact data is:

2, Prof. "Tsvetan Lazarov" Blvd., Sofia 1592, www.cpdp.bg.

If you want to lodge the complaint regarding the processing of your personal data to INFONOTARY, you may submit a complaint trough the above-mentioned contact details of the company or directly to a Data Protection Officer by e-mail: dpo@infonotary.com .