Operated by Evrotrust

PRIVACY POLICY APPLICABLE TO THE MOBILE APPLICATION „ID service, operated by Evrotrust”

Please carefully read this document. It is a Privacy Policy for use of the services accessible through the mobile application “ID, operated by Evrotrust” (Privacy Policy/the Policy).

This Privacy Policy constitutes an integral part of the Contract for Use of Services Accessible through the Application of Evrotrust Technologies AD (Contract). This Policy shall apply for use of services accessible through the mobile application “ID, operated by Evrotrust” (Application) in accordance with the Contract. Any changes to the Privacy Policy shall be published here.

1. WHO ARE WE AND HOW DO WE PROCCESS PERSONAL DATA?

In relation to provision of the services, available through the Application, Evrotrust Technologies AD (Evrotrust/ we), UIC: 203397356, registered address: Bulgaria, 1113 Sofia, Izgrev district, r.a. Iztok, 2 Nikolay Haitov Str. Entr. E, fl.2, correspondence address: Bulgaria, Sofia, 101 Tsarigradsko shose Blvd., fl. 6, telephone: (+359 2) 448 58 58, fax: (+359 2) 448 58 58, e-mail: office@evrotrust.com, website:https://www.evrotrust.com/, shall process personal data in compliance with this Policy.

In the processing of personal data Evrotrust complies with any personal data protection regulations including but not limited to 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 (the Regulation).

Pursuant to the Regulation personal data is any information relating to an identified natural person or a natural person who can be identified by name, an identification number, an online identifier, address, telephone number, e-mail address, etc.

Data processing is any operation or set of operations which is performed on personal data whether or not by automated means.

All terms and definitions used in the present Policy for which a definition is not provided herein have the meaning provided in the Contract, if not defined in the Contract, they shall have the meaning provided in the General Terms for the Provision of Trust, Information, Cryptographic and Other Services (General Terms) or in the respective Practice Statements and Policies of Evrotrust for the Provision of Trust Services (collectively referred to as “Practice Statements”); or if not defined in the above-mentioned documents shall have the meaning provided in the Regulation and the other applicable legal and regulatory acts.

2. FOR WHICH NATURAL PERSONS DO WE PROCESS PERSONAL DATA?

In relation to carrying out the activity of Evrotrust as a trust services provider, We process information regarding clients of Evrotrust – natural persons, who use Evrotrust services via the Application of Evrotrust (hereinafter referred to collectively as “client”/”You”) .

3. WHAT CATEORIES OF PERSONAL DATA DO WE PROCESS?

3.1. Data processed with regard to your registration in an Evrotrust Application

Identification data

In order to use the Evrotrust Application and the services You are required to register through the Application. Your registration in the Application requires You to:

1. enter Your contact data (mobile telephone number and e-mail address) and confirm their validity;
2. pass through a remote automated or semi - automated initial identification. The identification process is described in the Contract and the General Terms; and
3. confirm Your identification data collected during the identification process.

Biometric data as personal security codes

To ensure the highest possible level of security, the access to the Application, as well as activation/requesting services in the Application (e.g. applying for the issuance of qualified certificate for qualified electronic signature (QCQES), signing with QCQES) and confirming the execution of any legally valid electronic statements in or through the Application are confirmed by the biometric recognition functionalities supported by your device (e.g. fingerprint, facial recognition, etc.). When using the biometric recognition features supported by the device you use, your biometric data remains stored on your device and under your control and is not stored by Evrotrust. Apart from the activities requiring automated client identification (initial registration, account recovery upon reinstallation of the Application or provision of electronic identification service with additional automated client identification in real time included), Evrotrust does not process client’s biometric data. In the above-mentioned cases where biometric data is processed by Evrotrust, the processing is one-time and Evrotrust does not store such data in its systems, but only stores the result of the processing carried out (degree of identity).

Mandatory initial identification upon the Application activation

In order to use the trust services You are required to be unambiguously identified and Your identity to be checked. This necessity arises from the regulatory requirements to the services we provide as a qualified trust services provider. In order for You to be unambiguously identified we shall collect, process and store the following data relating to You:

- For automated identification: your names as per ID document, national identification number depending on the country-issuer of the ID document, ID document number, scanned copy of ID document, all automatically retrieved data from the machine readable part of the ID document or from the NFC chip, if the used ID document has such chip (including gender, date birth, expiry date, address); data for the validity of your ID document retrieved from the official databases of the competent authorities in the respective country-issuer of the ID document in case access to such databases is available in the jurisdiction of the country-issuer of the ID document (these data may include a photo of the official database of ID documents); record of video identification session and photos taken during the video identification session, mobile phone number, email address.
- For semi-automated identification: all above-mentioned data collected upon automatic identification, incl. a record of an identification video session with an operator from Evrotrust's Registration Authority and the information provided by You within the video session (answers to the questions asked by the operator).

Processing of biometric data and automated individual decision-making

When conducting automated or semi-automated identification, an one-time analysis and comparison of specific features of your face image (from a video session and photo as per your ID document) and indications whether in the video identification session participates a live person are performed. The analysis is performed to confirm with a sufficiently high level of identity, in accordance with the applicable legislation and standards, that the person in the video identification session, the photo from the ID document and the photos taken during the video identification session are of the same person. Specific aspect of the performed data processing by Evrotrust is that it is one-time and it is fully completed within the current identification session. Once the analysis of these data has been completed, the biometric data processed are automatically erased, retaining only the result in the form of a percentage of the degree of identity between the images analyzed.

Upon registration in the Application during the automated identification, a 3D FaceMap (Biometric Identifier) is generated. This Biometric Identifier is stored in a secure encrypted space (secure enclave/chip) only and exclusively on your device and is entirely under your control. Evrotrust does not in any way store the generated 3D FaceMap in its systems and does not have access to the secure enclave/chip space in your device. The Biometric Identifier does not allow the recovery of your biometric data in the opposite direction, but it allows, with each subsequent activation of the facial recognition function during a video identification session in the Application, to confirm in a unique and secure way that only you identify yourself in front of the Application.

When conducting automated identification, Evrotrust takes also a decision based solely on automated processing that has legally significant result for you – confirmation of your identification and issuance of a QCQES or respectively unsuccessful identification and refusal for remote issuance of a QCQES.

According to Art. 22 of the Regulation, you have the right not to be subject to such decision except with your explicit consent or when this is necessary for conclusion of a contract between you and the controller (in this case Evrotrust).

In case You wish to use the services of Evrotrust but do not wish your biometric data to be processed in the manner described in automated or semi-automated identification or to be subject to decision based solely on automatic data processing You may request services, which are provided upon present identification in an office of Evrotrust's Registration authority. If you consent to one-time processing of Your biometric data, to be identified and a QCQES to be issued in an automated manner, prior to the initial identification process You must grant Your explicit consent for the described processing.

For security reasons, avoidance of fraud and guaranteeing Your rights and interests after successful automated identification, the video identification session passes through an additional human verification from an operator of our Registration Authority. For the same reason, Evrotrust also stores all data, except biometric data, and records collected during an unsuccessful identification for a period of up to 2 (two) months after it has been conducted.

3.1. Data processed with regard to a secondary automated identification

3.1.1. Recovery of the access to an account in the Application

In order to be able to recover Your access to the Application, to Your account and to issued QCQES and to other services upon each reinstallation of the Application, regardless of whether reinstallation is carried out on the same device or on a new device, You need to go through an automated identification again and Evrotrust needs to process Your biometric data by analyzing specific features of Your face image within a new video identification session in the Application – a new, temporary 3D FaceMap is generated, which is compared to Your original 3D FaceMap (Biometric Identifier) stored in Your device or in a backup file, respectively, transferred by You upon reinstalling Your Application on a new device.

Prior to each start of such automated secondary identification, a screen for starting a video identification session appears in the Application and by pressing the "I'm ready" button, You give Your explicit consent to an automated processing of Your biometric data to start and the identification to be performed.

The access to the Application, to Your account and to Your already active services (for example, already issued QCQES) is recovered only in case of an exact match between two Biometric Identifiers – the original and current temporary 3D FaceMap.

The processing of biometric data is one-time, and immediately after the comparison of the two 3D FaceMaps, the Biometric Identifiers are automatically deleted from Evrotrust systems, and only the original 3D FaceMap (Biometric Identifier) is remain stored in a secure enclave space on Your device which Evrotrust does not have access to. The automatic secondary identification is the only way Evrotrust can ascertain that the person requesting recovery of access to Your user account is You and to recover it accordingly. If by that time You no longer consent to the processing of Your biometric data and a decision based on the automatic processing of Your

personal data, You will not be able to recover Your user account and use the Application through it. In this case, if You wish to use Evrotrust services, You can request those related to attendance identification at the office of our Registration Authority.

3.1.2. Document signing or e-identification (with highest level of security)

To ensure the highest possible level of security, the access to the Application, as well as activating/requesting services in the Application (e.g. applying for the issuance of QCQES, signing with QCQES, etc.) and confirming the execution of any legally relevant electronic statements in or through the Application are confirmed by the biometric recognition functionalities supported by Your device (e.g. fingerprint, facial recognition, etc.). When using the biometric recognition functionalities supported by Your device, the biometric data remain completely under Your control and do not reach, nor are stored by Evrotrust. Such data are processed only and exclusively on Your device.

In certain cases, however, a particular Relying Party (e.g. a bank where You apply for a service) may designate a specific transaction as requiring the highest level of security - e.g. the highest level when signing a document with QCQES or the highest level of security in electronic identification. In these cases, the standard functionalities for recognizing biometric data on Your device are not sufficient for signing the specific electronic document or for the provision of the electronic identification service, and automated secondary identification is performed in the manner described in item 3.2.1 above. Such identification is carried out only after Your confirmation in the Application to do so. If You do not consent to such processing of Your biometric data and to making decisions based on the automated processing of Your personal data, You can refuse to be identified within the particular session. Such refusal does not prevent You from continuing to use the Application, but according to Your relationship with the specific Relying Party this may result in the Relying Party's refusing to provide You with the service for the purposes of which it required signing the document or Your identification (e.g. remote bank account opening requiring Your secure identification) or may create the need to be identified by it in a different way (e.g. by a personal appearance before the Relying Party), etc.

A screen for starting a video identification session is displayed on Your screen and by pressing the “I’m ready” button, You confirm Your consent to proceed with it. Upon successful confirmation of Your identification by matching the compared Biometric Identifiers, You successfully confirm the signing of the relevant electronic document and / or Your electronic identification to the Relying Party.

As soon as the video identification session is completed, the Biometric Identifiers are automatically deleted from the Evrotrust systems and only the original 3D FaceMap (Biometric Identifier) remain stored in the secure enclave in Your device, to which Evrotrust does not have access. The Relying Party does not have access to the Biometric Identifiers.

3.2. Data processed in case of changes in facial biometrics

In the event of a change in Your facial biometrics (e.g. as a result of trauma, surgery, etc.), it would be impossible to perform Your automated secondary identification in the manner described in item 3.2 above. In this case, Your access to the Application and Your account can be recovered

if You have an updated ID document. For this purpose, You will need to update the information regarding Your ID document and go through the process of mandatory initial identification according to item 3.1 above.

3.3. Data contained in the QCQES issued by Evrotrust and their publication

The content of the issued QCQES is in compliance with the applicable European standards. QCQES issued by Evrotrust will contain Your names or pseudonym of Your choice, country, information about start and end date of validity, Your public key, information on issuer and data that serves the recognition and verification of the certificate validity by the relying parties.

When issuing an attributive QCQES in addition to the data indicated above based on Your assignment Evrotrust may include information about Your national identification number, ID document number, etc., as well as information such as date of birth, gender, ID document expiry date and other data retrieved from NFC chip of Your ID document and/or the database of the primary data controllers in the jurisdiction of the country-issuer of Your ID document. What data are included as per Your assignment in an attributive QCQES depend on what data You wish Evrotrust to certify to the Relying Parties before which you will use this QCQES.

Pursuant to the applicable legislation every qualified trust services provider keeps a register of the QCQES issued by it as well as for all terminated or suspended QCQES. This is done for the purpose of all Relying Parties to be able to check the certificates validity and who is the signatory. Evrotrust provides a functionality for validity check of the QCQES issued by it. The attributive QCQES are not available in our register.

3.4. Data, processed when you sign documents through the Application of Evrotrust

For every signing of documents through the Application Evrotrust stores information in the form of records/ logs for the fact and time of signing through the functionalities of the Application and the fact and time of sending and receiving of the documents, together with system identification numbers of the client and the Relying Party (sender of document for signing/ recipient of a signed document) respectively.

In accordance with the requirements applicable (legislation and standards) to the provision of trust services, those records/ logs are stored for a period of 10 years regardless of the termination of Your registration in the Application.

When using the Application Evrotrust has no access to and does not in any way keep the documents signed by You through the Application. For the period for which You have an active registration and access to the Application the documents signed by You may be accessed and stored by You on Your own storage through functionalities of the Application. In connection with the above, it is recommended that after signing You store the documents signed by You through the functionalities in the Application. Evrotrust is not responsible should You not have access to documents signed by You, whereas they are under the control of the Relying Party.

3.5. Data processed when providing the qualified storage of qualified electronic signature/ stamps service.

Your private keys are stored in a special Hardware Security Module – HSM in an encrypted form which can be decrypted only by You via the Application by the biometric recognition functionalities supported by your device (e.g. fingerprint, facial recognition, etc.).

3.6. Data processed upon using the electronic identification (e-identification) service

The e-Identification service enables you to identify yourself before third parties – Relying Parties (e.g. a bank), in cases where signing a contract, using remote services of the Relying Party, etc. In these cases, the Relying Party sends to Evrotrust data that identifies You (mobile phone number or email address) with a request for You to be identified. In the Application You are notified of each Relying Party that requests You to be identified before it. In order to activate the e-identification service, you need to carefully review the personal data required from You and to confirm through the Application that you wish to be identified before the specified Relying Party. As a result, an electronic document is generated – a statement for submission of personal data, that contains information about Your personal data attributes that the Relying Party has requested to be verified (certified). After you confirm through the Application the signing of the statement for submission of personal data, Evrotrust issues to You a one-time attributive QCQES with the content requested by the Relying Party for identification purposes only. This attributive QCQES contains all the personal data for which Evrotrust has ensured that are up-to-date and has verified with permitted by the law means in accordance with Regulation (EU) 910/2014. With the attributive QCQES you are signing remotely the document – statement of submission of personal data by You and serves only for the purposes of Your identification as far as the attributive QCQES engages Evrotrust's liability for the validity of the data entered in this QCQES. This document may include your name, national identification number, copy of your ID, etc. for the needs of the requested service. If you agree to identify Yourself before the Relying Party with the data specified in the document, you need to sign it with your attributive QCQES issued to You for this purpose and to assign to Evrotrust to send the signed document to the Relying Party.

The e-Identification service also includes as an integral part the sending of the above document signed by You to the Relying Party. Therefore, in these cases, Evrotrust also processes and stores the information under item 3.5 above, which is intended to evidence the sending, receiving and signing of documents through the Application. This information will be kept for a period of 10 years.

3.7. Data processed with regard to the payment of the provided services

For the purposes of payment for the services provided and determination of the due remunerations for the services provided, Evrotrust processes information on the type and volume of the services provided, including information on the number of signings and the time of their provision, as well as information on the Relying Party in the relations with which the respective service has been used (in the cases where the services are paid for by the Relying Parties).

In case You make payments to us for the use of services, we will further process the following information relating to you: VAT number (for natural persons with VAT number), method of payment, incl. the account from which the payment was made, information on payments due and made by You and data contained in the tax and accounting documents in accordance with the applicable legislation.

3.8. Other information we collect by automatic means

In order to ensure the proper functioning and security of the Application and our services upon installation and use of the Application, Evrotrust automatically collects information about the type of device, the type of operating system used by the device, the language settings You have chosen, the number of electronic statements made and the number of unsuccessful attempts to use the services (if any).

In addition, Evrotrust keeps records/ logs of all significant events in its systems for a period of a minimum of 1 (one) year unless another term has been explicitly provided for in the Contract, the General Terms or in this Privacy Policy.

4. FOR WHAT PURPOSES DO WE PROCESS YOUR PERSONAL DATA?

Evrotrust collects, stores and processes the information specified in item 3 above for the purposes of this Policy, the Contract and the General Terms. Depending on the legal basis for processing, these purposes may be:

- purposes related to compliance with legal obligations of Evrotrust;
- purposes related to and/or necessary for the performance of the contracts concluded between You and Evrotrust or for taking steps upon your request prior to the conclusion of such contract;
- purposes of the legitimate interest of Evrotrust or of third parties;
- purposes for which you have given You consent to processing of Your data.

4.1. The purposes for personal data processing by Evrotrust related to compliance with legal obligations include:

- fulfillment of the regulatory requirements applicable to the provision of trust services, incl. ensuring Your secure identification, checking the authenticity of the data you provide, checking the validity of your ID document, including the content required in certificates issued by Evrotrust, etc.;
- fulfilment of the regulatory requirements for retention, publication, provision of or access to information in relation to the activity of Evrotrust as a qualified trust services provider;
- fulfilment of the obligations of Evrotrust stipulated in the law for reproducing and evidencing of the electronic statements made by You;
- compliance with the applicable tax and accounting legislation;
- other activities for fulfillment of legal obligations of Evrotrust related to the provision of information to competent state and judicial authorities or for provision of assistance with

inspections by competent authorities or legal audits related to the regulated activity of Evrotrust as a trust service provider.

All information relevant to and all data created or received by Evrotrust in connection with the process of identification and registration of a client and/or the conclusion of the Contract(including evidence of its conclusion) are recorded and stored by Evrotrust for the entire duration of the respective contract and for a period of 10 (ten) years after its termination. Within this period, information on each issued, suspended and terminated certificate by Evrotrust is stored, as the term begins as of the termination of the certificate. The same term applies to information created or received by Evrotrust in connection with the process of providing qualified storage of signature/ stamp. This information will be stored for the period specified hereunder, including after Evrotrust has ceased its activity. This information is stored in order to fulfill the legal obligations of Evrotrust under Art. 24 Para 2, letter “h” of Regulation (EU) № 910/2014 and the standards applicable to its activity and with a view to providing evidence in legal proceedings and ensuring continuity in the provision of the service.

For the above-mentioned purposes we process all categories of personal data specified above.

4.2. The purposes for personal data processing related to and/or necessary for the performance of the contract or for taking steps upon client’s request prior to the conclusion of contract with Evrotrust include:

- activities for carrying out Your registration;
- activities for provision of the services through the Application;
- contacting You in regards the services provided;
- fiscal and accounting activity and administration, processing and collection of payments related to the services;
- for the above-mentioned purposes we process all categories of personal data specified above.

4.3. The purposes for personal data processing in connection with the legitimate interest of Evrotrust or of third parties include:

4.3.1. Legitimate interest – exercise and protection of legal rights and interests of Evrotrust; and assistance in exercising and protecting the legitimate rights and interests of clients; of other entities associated with Evrotrust; of the Relying Parties; of employees of Evrotrust; of persons processing personal data on behalf of Evrotrust; and of Evrotrust’s business partners:

- establishment, exercise and protection of legal claims of the above-mentioned persons incl. judicial remedy, including the lodging of complaints, signals, etc. to the competent state and judicial authorities, incl. reproduction of the retained information in the scope required for these purposes;
- taking actions to suspend the provision of services in case of breach of the Contract, the General Terms and non-compliance with Evrotrust’s Practice Statements;
- administration and processing of filed complaints, reports, requests, etc.;

- collection of debts owed to Evrotrust, including by outsourcing to third parties.

4.3.2. Legitimate interest – ensuring the services as well as the normal functioning of the Application:

- maintenance and administration of the services and the Application;
- taking measures against malicious acts against the security and normal functioning of the Application;
- establishment and resolving of technical problems related to the functionality of the Application;
- creation of secure environment for exchange of messages between the client, Evrotrust and the Relying Party;

For the above-mentioned purposes we process all categories of personal data specified above.

4.4. Explicit consent

Your data may be processed based on Your explicit consent, the processing in this case is specific and to the extent and scope provided in the respective consent. Such purposes include:

- automated and semi-automated identification through Application of Evrotrust in order to ensure Your secure identification necessary for the use of the provided services;
- Secondary automated identification:
    - For the purposes of providing the capability to securely restore Your access to an account in the Application;
    - For the purposes of providing the capability for signing documents or for electronic identification (at the highest level of security) to a specific Relying Party which has requested such a level of security.

You grant Your explicit consent for the processing of personal data activities specified above by confirming the Declaration of consent in the Application. Upon each start of data processing for the purposes of automated secondary identification, a screen for starting a video identification session appears in the Application and by pressing the “I'm ready” button, You express your explicit consent to an automated processing of Your biometric data to start and the identification to be performed.

- Participate in a survey of your service satisfaction if you have agreed to participate in such.

5. WITH WHOM DO WE SHARE YOUR PERSONAL DATA?

Evrotrust does not provide your personal data to third parties in any other way except in the cases described in this Policy, the Contract, the General Terms or provided for by law.

Evrotrust may disclose Your personal data to third parties:

5.1. if this is necessary to comply with a legal obligation of Evrotrust, for example, when providing information by Evrotrust to:

- competent state, municipal or judicial authorities;
- auditing bodies;

5.2. if this is necessary for the provision of the services such as:

- banks and payment service providers in connection with payments made;
- Relying Parties before whom You wish to be identified through the Application;
- persons to whom you send documents for signature or signed documents using our services;
- post and telecommunication operators for carrying out the communication between us;

5.3. if this is necessary for protection of the rights and the legal interests of Evrotrust, of third parties or Yours. In these cases, we may provide Your personal data to:

- state, municipal and judicial authorities;
- private and state bailiffs;
- lawyers;
- notaries.

5.4. who act as data processors on behalf of Evrotrust such as cloud services provider, Evrotrust's Registration Authority (when this activity is assigned to a third party), accounting services provider, etc.

Evrotrust uses subcontractors and service providers as dedicated data centers for reliable and secure co-location of server and network equipment, cloud systems and service providers, automated identification service providers, other IT services, etc. In its relations with subcontractors and service providers, Evrotrust requires them to strictly comply with its instructions in accordance with this Policy.

5.5. in the cases where You have given Your explicit consent;

5.6. in other cases provided for by the law.

6. TRANSFER OF PERSONAL DATA OUTSIDE THE EU/EEA.

6.1. The data is processed on the following service provider's servers only on our behalf and according to our instructions:

Amazon Web Services EMEA SARL
38 avenue John F. Kennedy,
L-1855 Luxembourg

At AWS, according to agreements concluded with us, the data is encrypted and exclusively processed on data servers in the European Union.

6.2. In cases where you enter into relations with Relying Parties who are established outside the EU, the signing by you of documents sent by them for signature and their sending back to

them, as well as your e-identification before such Relying Parties, by the use of the services in the Application, are respectively related with sending/ provision of Your data to the respective Relying Party that is established in a country outside EU. Such sending/ provision is necessary for the performance of our contractual obligations to you and is entirely under your control, as you and only you decide to which Relying Party to sign documents by using our services.

7. FOR WHAT PERIOD DO WE STORE YOUR PERSONAL DATA?

7.1. Evrotrust processes and stores information about You until it achieves the relevant purposes for which the information has been collected and is being processed.

7.2. In accordance with its internal rules and procedures and the applicable law, Evrotrust processes and stores information about you within the following terms:

Types of data	Storage period
Information contained in the certificates issued by Evrotrust in accordance with Art. 28 of Electronic Document and Electronic Trust Services Act (EDETS) and published in the electronic registers	For the entire period of validity of the certificate and a period of 10 years after its termination.
Information collected and stored in connection with the provision of trust services as: 1.All information relevant to and all data created or received by Evrotrust in connection with the process of identification and registration of a client and/or the conclusion of the Contract (including evidence of its conclusion); 2.Video session records (automatic and via operator) for the purposes of client's identification; 3.Information on signed electronic documents as metadata/description of documents; 4. History of signing; 5. Audit logs with information about documents sent and received; 6. Information contained in the communication with the clients in regards the services.	All information collected and stored in connection with the provision of trust services will be kept for the entire duration of the service provision and for a period of 10 (ten) years after its termination.
Information related to the use of the qualified electronic signature storage service.	For the period of validity of the issued QCQES.
Financial and accounting documents; invoices; other information related to tax and social insurance control.	Up to 10 /ten/ years from the beginning of the year following the year in which payment of the obligation for the relevant year is due.
System logs of the application. Logs related to security, technical support, etc. (may contain information such as date and time, IP address, URL, browser and device version information)	10 /ten/ years from the generation of the relevant log. Up to 10 /ten/ years from the beginning of the year following the year in which

	payment of the obligation for the relevant year is due.
Data and records collected in an unsuccessful identification.	2 (two) months after it was made.10 /ten/ years from the generation of the relevant log.
Biometric data processed during automated or semi-automated initial identification in the process of registration and activation of the Application. Biometric data processed during automated or semi-automated secondary identification;	One single time during the respective remote identification video session (maximum duration of the video session up to 5 minutes).
Data processed based on your explicit consent, except the biometric data (see above).	From the moment the consent was given to its withdrawal from the data subject. The storage period shall be no longer than the storage period specified in the respective consent (if such a storage period is explicitly specified therein) and no longer than the period necessary to achieve the relevant purposes for which the personal data has been collected and is being processed.

The personal data listed in this Policy may also be processed for longer periods of time than the ones specified above if this is necessary to achieve the purposes set forth therein or to protect the rights and/or legitimate interests (including through judicial remedy) of Evrotrust or of third parties or if the legislation in force provides for processing of the data for a longer period.

8. WHAT ARE YOUR RIGHTS AND HOW YOU CAN EXERCISE THEM?

In connection with the personal data processing we carry out, You have the following rights under the Regulation and the applicable personal data protection legislation:

8.1. Право на информации

You have the right to obtain information about the processing of your personal data by us, as this information is contained in this Policy;

8.2. Right of access

You have the right to obtain confirmation as to whether or not Your personal data are being processed, access to them and information on the processing and Your rights in this regard.

8.3. Right to rectification

You have the right to request the rectification of Your personal data in case they are incomplete or inaccurate.

8.4. Right to erasure

You have the right to request erasure of Your data, if the grounds for doing so provided for in the Regulation are in place.

8.5. Right to restriction in relation to the data processing

The Regulation provides for the possibility to restrict the processing of your personal data if the grounds for doing so are in place.

8.6. Right to notification of third parties

You have the right to request from us to notify third parties to whom your personal data has been disclosed of any rectification, erasure, or restriction of the processing of your personal data, unless this is impossible or requires disproportionate effort on our part.

8.7. Right to data portability

You have the right to receive the personal data that are concerning You and that You have provided to us in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance on our part.

The right to data portability applies where both of the following conditions are met:

- the processing is based on consent or on contractual obligation; and
- the processing is carried out by automated means.

If technically feasible, You shall be entitled to have Your personal data directly transmitted from Us to another controller. The right to data portability may be exercised in a way that does not adversely affect the rights and freedoms of other persons.

8.8. Right not to be subject to a decision based solely on automated processing

You have the right not to be subject to a decision based solely on automated processing including profiling, which produces legal effects concerning You or similarly significantly affects You, unless the grounds provided for doing so in the applicable personal data protection legislation are in place and appropriate safeguards to protect your rights, freedoms and legitimate interests are provided.

Upon registration in the Application through initial automated identification, as well as upon conducting secondary automated identification, on the basis of your explicit consent and in view of conclusion of Your contract with Evrotrust a decision based solely on automated processing of your personal data (incl. biometric data) is made which has legally significant result for You –

confirmation of Your identification and issuance of QCQES. The appropriate safeguards provided for your rights, freedoms and legitimate interests in this regard are as follows:

- If you do not wish to be subject to a such decision, you may pass use the services of Evrotrust which are provided upot present identification at an office of Evrotrust's Registration Authority (e.g. issuance of QCQES on an USB drive);
- In case of unsuccessful automated identification – human intervention through real-time video conference call via Application of Evrotrust between You and operator of Evrotrust's Registration Authority.

In addition to safeguard your rights and interests after successful automated identification, the record from the video identification shall passed through an additional human verification by an operator of the Registration authority. For the same reason, Evrotrust stores all collected data and records during an unsuccessful identification for a period of up to 2 months from the date when it was made.

8.9. Right to withdrawal of consent

You have at any time the right to withdraw your consent to personal data processing if the respective processing is based on the consent given by You. Such withdrawal does not affect the lawfulness of processing based on consent before its withdrawal.

To withdraw the consent given in Application Version 2.0, You need to deactivate your account and stop using the Evrotrust services available through this Application. If, after withdrawing Your consent, You wish to continue using the services of Evrotrust, You may request services that require present identification (e.g. issuance of a QCQES on an USB drive) after you are identified in person at an office of Evrotrust's Registration Authority. When you deactivate your account, access to all services activated by You in the Application is terminated (e.g. remotely issued QCQES is terminated).

8.10. Right to object

You have the right to object at any time and on grounds relating to Your particular situation, to processing of Your personal data which is based on public interest, exercise of official authority or Evrotrust or of a third party.

In the event of such an objection, we will examine Your request and, if justified, we will comply with it. If we consider that there are compelling legitimate grounds for the processing or that it is necessary for the establishment, exercise or protection of legal claims, we will inform You accordingly.

8.11. Exercise of rights

The rights described above may be exercised at any time using the functionalities available in the Application, or you may send a written request to the Evrotrust's DPO – by mail to the contact address or by e-mail to the email address specified in item 1 of this Policy, in accordance with the procedure laid down by the applicable legislation.

8.12. Right to lodge a complaint with a supervisory authority

You have the right to lodge a complaint with a supervisory authority, in particular in the Member State of Your habitual residence, place of work or place of the alleged infringement if You consider that the processing of Your personal data infringes this Regulation or other applicable personal data protection requirements.

The supervisory authority in the Republic of Bulgaria is the Commission for Personal Data Protection, address: Sofia 1592, 2 Prof. Tsvetan Lazarov Blvd., Website: https://www.cpdp.bg/. You can find information about the supervisory authorities of other Member States here.

9. HOW DO WE PROTECT YOUR PERSONAL DATA?

We will take all necessary steps, including technical and organizational measures tailored to the level of risk to the processing carried-out by us to safeguard the security of Your personal data so as to prevent accidental or unlawful destruction, loss, alteration, unlawful disclosure, access, or other illegal or undesirable event that could endanger the security of personal data processed by us.

10. WHO CAN YOU CONTACT IN REGARDS YOUR PERSONAL DATA PORCESSING AND EXERCISE OF YOUR RIGHTS? OUR DATA PROTECTION OFFICER

You may address all your requests and questions relating to the protection of your personal data and the exercise of your rights under personal data protection law to our DPO:

telephone: (+359 2) 448 58 58
e-mail address: dpo@evrotrust.com
Address: Sofia, 101 Tsarigradsko shose Blvd. fl.6

11. CHANGES TO THE POLICY

We may update this Policy from time to time in order to reflect any changes in the processing of your personal data or to comply with changes in current legislation.
All changes which we may further make will be published in the Application as well as on the website: www.evrotrust.com.

The Privacy Policy is in force as of 01.12.2020, last update on 01.12.2020.

This document has been published on Evrotrust's website on the internet in Bulgarian and in English language. In case of any discrepancy between the Bulgarian and the English text, the Bulgarian text takes precedence.