

Please read this document carefully. It is the Privacy Policy Applicable to the Trust, Information, Cryptographic and Other Services Provided by Evrotrust (hereinafter, **the Privacy Policy** or **the Policy**).

This Privacy Policy forms an integral part of the General Terms and Conditions of the Contract for Trust, Information, Cryptographic and Other Services (hereinafter, **the General Terms and Conditions**) of Evrotrust Technologies AD. The Privacy Policy is available on the Evrotrust website [here](#).

This Privacy Policy is applicable to the activities carried out by Evrotrust in the provision of services subject to the General Terms and Conditions. In respect of certain of its services, Evrotrust may provide for and implement, in addition, special personal data protection policies relating to the processing of personal data by Evrotrust in the provision of these services. In the event of a conflict between this Privacy Policy and such special policies, the special policies shall prevail, but only in respect of processing activities related to the provision of the relevant services to which those policies relate. In the case of gaps in the special policies, the provisions of this Privacy Policy shall apply.

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

Depending on the services you use and the country you are located in or of which you are a citizen, your personal data is processed by Eurotrust Technologies AD, UIC: 203397356, business address: 251G Okolovrasten pat Str., MM Business Center, 5<sup>th</sup> floor, 1766 Sofia, Bulgaria, tel.: +359 2 448 58 58, e-mail address: [support@evrotrust.com](mailto:support@evrotrust.com), website: <https://www.evrotrust.com/> (hereinafter, **Evrotrust** or **we**), and/or by its affiliate company providing the services in the relevant country, as specified in item 10 'Special rules' below.

When processing personal data, Evrotrust complies with all applicable personal data protection regulations applicable to its activities, including, but not limited to, Regulation (EU) No 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 (hereinafter, **the Regulation**).

All terms and definitions used in this Policy for which no definition is given here shall have the meaning given to them in the General Terms and Conditions or in the relevant Evrotrust policies and practices applicable to the provision of the respective qualified trust service (hereinafter, **the Policies and Practices**), or, if not defined in the those documents, shall have the meaning given in the Regulation and in other applicable laws and regulations.

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

In relation to the performance of the activities of Evrotrust as a provider of qualified and unqualified trust services, and other information society services, we process information on the following data subjects (hereinafter, **Data Subject(s)** or **Subject(s)** or **you**):

- (1) Natural persons who are Subscribers of Evrotrust;
- (2) Natural persons who act on behalf of Subscribers of Evrotrust and natural persons designated as contact persons by legal entities who are Subscribers of Evrotrust;
- (3) Natural persons who submit inquiries (including by phone call), requests, signals, complaints or other correspondence to Evrotrust;
- (4) Natural persons whose information is contained in inquiries (including by phone call), requests, signals, complaints or other correspondence addressed to Evrotrust.

## **3. WHAT CATEGORIES OF PERSONAL DATA DO WE PROCESS?**

### **3.1. Data processed in connection with your identification for the purpose of requesting Evrotrust services and entering into a contract with us**

#### **3.1.1. Data processed when requesting services and entering into a contract with us in person**

Some of Evrotrust services may be requested in person at our office or at the office of a Registration Authority. In such cases, we may process the following data:

- Your identification data: full name (according to an identity document); data from an identity document (national identification number depending on the issuing country of the identity document, number, date of issue, date of validity and issuer of the identity document, sex, date of birth; address); image of the identity document, data retrieved during the performance of an official verification of the validity of your identity document from the official databases of the competent authorities in the relevant issuing country of the identity document

(if access to such databases is available in the jurisdiction of the issuing country of the identity document) and/or data retrieved from the machine readable part or from the NFC chip of the identity document (this may include a photo from the official identity document databases); signature;

- Contact details - mobile phone number, e-mail address and postal address;
- If applicable, data on the Subscriber you represent and on your representative power (type, period, restrictions, change, copy of power of attorney, power of attorney details, etc.), position, official contact details (telephone number and e-mail address);
- If applicable, personal data contained in documents about a legal entity Subscriber submitted to Evrotrust (e.g. documents certifying the establishment of the legal entity or its current status, etc.) in connection with its identification as a Subscriber;
- If applicable, information before which person - external Registration Authority of Evrotrust, the identification is performed.

### **3.1.2. Data processed in relation to the registration and/or the identification within Evrotrust's mobile application**

#### **3.1.2.1. Registration in Evrotrust's mobile application**

In order to use Evrotrust's mobile application (hereinafter, **the Mobile Application** or **the Application**) and the services provided through it, you must register in the Application. During the registration process in the Application, you provide the following data, which we process as described below:

- Your nationality
- Your mobile phone number (which you subsequently confirm by entering the code received for this purpose on your mobile phone number);
- A personal security code created by you (PIN code, and if you wish - a login password, according to the instructions in the Application).

**Important!** Your PIN code and password are strictly personal and are not stored by Evrotrust in an unencrypted ('clean') form, nor in the Application itself. Therefore, it is not possible to recover a forgotten PIN code, as it is stored by Evrotrust only in encrypted form, in a way that allows it to be used only by you. If you have forgotten your PIN code, you may restore your ability to use the

Application and services in accordance with the procedure provided for in the General Terms and Conditions.

Depending on the functionalities of your device on which the Application is installed, biometric data can be attached to your personal security code – fingerprint, face shape, etc., which you can use for convenience as a personal security code. Such is, for example, the FaceID functionality of Apple, etc. When using such functionalities, your biometric data remains solely under your control and within your device always and at all times. It is not processed and stored by Evrotrust. You can stop using such functionalities at any time.

### **3.1.2.2. Identification through the Evrotrust's mobile application**

To use the trust services provided by Evrotrust you need to be unambiguously identified and your identity needs to be verified and confirmed. This necessity arises from the regulatory requirements applicable to the services we provide as a qualified trust services provider. In order for you to be unambiguously identified we collect, process and store the following data relating to you:

(a) In the case of automated identification: your names as per your identity document, national identification number depending on the country of which you are a citizen, identity document number, image of the identity document, all automatically retrieved data from the machine readable part of the identity document (including gender, date birth, expiry date); data obtained from the databases of primary data controllers (Ministry of Interior, Ministry of Regional Development and Public Works, etc., depending on the country issuing the identity document) obtained following *ex officio* checks on the validity of your identity document, which include a photo from the official database of identity documents - in case of connectivity to such databases; recording of the automated video identification and photos taken during the automated video identification carried out; metadata.

(b) In the case of semi-automated identification: all above-mentioned data collected in the context of automatic identification, as well as, where applicable, a recording of the identification video session carried out 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).

(c) In the case of in-person identification in an office of Evrotrust's Registration Authority: data as described in item 3.1.1.

**3.1.2.2.2.** When conducting automated or semi- automated identification, one-time analysis of your biometric data is performed. The analysis is performed to confirm with a sufficiently high degree of matching, in accordance with the applicable legislation and standards, that the person in the video identification session, the person on the photo from the identity document and on the photos/captures taken during the video session are the same person. In this process, a liveness check is performed to ensure that a real and alive human being is taking part in the video session. Once the analysis of this data is complete, the processed biometrics are automatically erased, retaining only the result in the form of a percentage of the degree of matching between the analyzed images. When conducting an automated identification, Evrotrust takes a decision based solely on automated processing that has significant legal consequences for you - confirmation of your identification and issuance of a Qualified Certificate for Qualified Electronic Signature (hereinafter, **QCQES**). You have the right not to be subject of a such decision except when you have provided your explicit consent or when this is necessary for the conclusion of a contract between you and Evrotrust.

In case you wish to use the services but do not wish your biometric data to be processed in the described manner during an automated or semi-automated identification process, nor to be subject to decision based solely on automatic data processing, you may be identified in-person (with physical presence) in an office of Evrotrust's Registration Authority. If you consent to the one-time processing of your biometric data, and to being identified and having an QCQES issued to you in an automated manner, you need to give your explicit consent for this processing prior to the identification process.

**3.1.2.2.3.** For reasons related to security, fraud prevention, and safeguarding of your rights and interests, after successful automated identification, the video identification session may go through an additional human verification by an operator of our Registration Authority.

### **3.1.2.3. Evrotrust's SDK Modules for integration**

The rules set in this Privacy Policy regarding the Evrotrust Mobile Application and the services provided via the Application, including what is described in this item 3.1.2, are relevant and applicable in the event the identification is performed and the corresponding services are requested and provided via Evrotrust SDK module integrated in applications of third parties - clients and partners of Evrotrust.

### **3.1.3. Data processed in relation to remote identification via web interface**

**3.1.3.1.** For some of its services, Evrotrust can provide you the possibility to conclude the contract by means of a web interface functionality, available independently or as a built-in functionality in a mobile application or web interface (website) (together hereinafter, **the Electronic Channel**) of a third party who is a Relying Party. In these cases, we collect, process and store the following personal data relating to you:

(a) In the case of automated identification: your names as per your identity document, national identification number depending on the country of which you are a citizen, identity document number, image of the identity document, all data automatically retrieved from the machine readable part of the identity document (including gender, date of birth, expiry date); data obtained from the databases of primary data controllers (Ministry of Interior, Ministry of Regional Development and Public Works, etc., depending on the country issuing the identity document) obtained following *ex officio* checks on the validity of your identity document, which include a photo from the official database of identity documents – in case of connectivity to such databases; video recordings and photos/captures taken during the identification session.

(b) In the case of semi-automated identification: all above-mentioned data collected in the context of automatic identification, as well as, where applicable, a recording of an identification video session carried out with an operator from Evrotrust's Registration Authority, and the information provided by you during the video session (answers to questions asked by the operator).

(c) In the case of in-person identification in an office of Evrotrust's Registration Authority: data as described in item 3.1.1.

**3.1.3.2.** When conducting automated or semiautomated identification, one-time analysis of your biometric data is 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 person on the photo from the ID document and on the photos/captures taken during the video session are the same person. In this process, a liveness check is performed to ensure that a real and alive human being is taking part in the video session. Once the analysis of this data is complete, the processed biometrics are automatically erased, retaining only the result in the form of a percentage of the degree of matching between the analyzed images. When conducting automated identification, Evrotrust takes a decision based solely on automated processing that has significant legal consequences for you – confirmation of your

identification for the purpose of using the respective trust service. You have the right not to be subject of a such decision except when you have provided your explicit consent or when this is necessary for the conclusion of a contract between you and Evrotrust.

In case you wish to use the services but do not wish your biometric data to be processed in the described manner during an automated or semi-automated identification process, nor to be subject to decision based solely on automatic data processing, you may be identified in-person (with physical presence) in an office of Evrotrust's Registration Authority or of the respective Relying Party, if applicable. If you consent to the processing of your data in the described manner, you need to give your explicit consent for this processing prior to the identification process.

**3.1.3.3.** For reasons related to security, fraud prevention, and safeguarding of your rights and interests, after successful automated identification, the video identification session may go through an additional human verification by an operator of our Registration Authority.

#### **3.1.4. Data processing in relation to the request of services through an Electronic Channel of an external Registration Authority of Evrotrust**

Evrotrust provides you the opportunity to request the conclusion of a contract and the use of services after you have been previously identified by a third party - external Registration Authority of Evrotrust (e.g. bank), in the context of another activity carried out by the Registering Authority (e.g. a banking activities) and in the presence of continuity in the use of the Registration Authority's services in connection with which you were identified. Previous identification under these conditions for the purposes of requesting and using Evrotrust's services may be performed in-person (with your physical presence) before a representative of the respective Registration Authority or remotely, through application by the Registration Authority of a certified method for remote identification of Evrotrust which meets the requirements of Art. 24, para. 1a, item (c) of 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 (hereinafter, **Regulation (EU) No 910/2014**). When the requested services do not include the issuance of a qualified certificate, identification may be performed by the Registration Authority in another manner permitted by applicable law. In all cases, the conclusion of the contract takes place after you confirm the use of the relevant service by entering a PIN code or by clicking on an active link sent in an SMS message to your mobile

phone number. The PIN code and the secret link are valid and can be used only once, within a limited period of time, and only for the purpose for which they are provided.

In these cases as described under this item 3.1.4, Evrotrust does not receive all the data provided by you during the identification by the Registration Authority, but only a minimum set of data, as follows:

(a) in the case of in-person identification (with physical presence): data necessary for your identification for the purposes of providing the specific requested service, as described in this Policy, as well as information before which person - external Evrotrust Registration Authority - the identification was carried out;

(b) in the case of identification using a certified method for remote identification of Evrotrust meeting the requirements of Art. 24, para. 1a, item (c) of Regulation (EU) No 910/2014: the data under item (a) above, as well as data necessary to establish the correct application of the method for identification, including logs (such as logs for time) of the performed steps in the process, photos and video recordings of the automatic identification, other data depending on the specific technical implementation of the method;

(c) in the case of remote identification for the purposes of services that do not include the issuance of a qualified certificate: data necessary for your identification for the purposes of providing the specific requested service as described in this Policy, as well as information before which person - external Registration Authority of Evrotrust, the identification was carried out.

In all those cases, Evrotrust acts as a data controller and is responsible solely for the data received from the relevant third party - the Registration Authority, for the purposes of providing the trust service requested by you.

In these cases, the relationship between you and the Registration Authority in relation to the processing of your personal data, including the categories of data collected during the identification, the purposes, terms and methods of its processing, as well as the compliance with the other requirements of the applicable legislation, shall be settled between you and the respective Registration Authority.

### **3.1.5. Data processing of other information in relation to the conclusion of a contract**

In addition to the information contained in items 3.1.1 – 3.1.4 above, in connection with the conclusion, amendment, performance and termination of a contract for the provision of our services, we may also process the following personal data:



- information about the contract: type of contract; date of conclusion; terms and conditions of the contract; information and documents related to the amendment, performance or termination of the contract (notices, date, legal grounds, accompanying documentation, etc.); amendments to the contract; other aspects relevant to the validity, conclusion and performance of the contract; notifications and other documents and information related to the contract, incl. any documents and information related to actions (legal and factual) taken and statements made in connection with the contract;
- correspondence and other communication related to the contract; information contained in or related to inquiries, offers, reviews/feedback, complaints, claims, etc.
- other information created or exchanged during the negotiation, conclusion, amendment, performance and termination of contracts.

### **3.2. Data processed in connection with the issuance of qualified and non-qualified certificates for electronic signature**

When issuing a qualified certificate for electronic signature, Evrotrust processes the personal data required for identification for the purpose of requesting a service from Evrotrust and entering into a contract with us, described in item 3.1 above.

For the purposes of the issuance of short-term qualified certificate for electronic signature following identification carried out by an external Registration Authority of Evrotrust according to item 3.1.4 above, the data under item 3.1 includes at least your names; the country issuer of your identity document; your national unique identification number, if any, in accordance with the technical specifications for the purposes of the cross-border identification, which number remains unchanged for as long as possible (for example, in Bulgaria this is the unified citizen number (EGN)), your identity document number, your mobile phone number and e-mail address.

For the purposes of the issuance of a short-term non-qualified certificate for electronic signature following identification carried out by an external Evrotrust Registration Authority according to item 3.1.4 above, the data under item 3.1 above includes at least your name on your identity document, your personal identification number (or other national identification number depending on the country of your citizenship), your identity document number, the country - issuer of the identity document, your phone number.

The content of the qualified and non-qualified certificates for electronic signature issued by Evrotrust is in accordance with the applicable European standards. A certificate issued by

Evrotrust will contain your name or a nickname chosen by you, country, information about the start and end dates of the certificate's validity, your public key, information about the issuer, as well as data for the purposes of recognition and verification of the validity of the certificate by the Relying Parties. In addition, the certificate may also contain information about a legal entity with which you have a legal relationship. At your express request, the issued certificate may also contain information about your unique identification number, if any, in accordance with the technical specifications for the purposes of the cross-border identification, which remains unchanged for as long as possible (for example, in Bulgaria this is the unified citizen number (EGN)).

For the purposes of the issuance of an attributive qualified certificate for qualified electronic signature (hereinafter, **attributive QCQES**), in addition to the abovementioned data, Evrotrust may, at your assignment, include information about your national identification number, identity document number, VAT number, or other, as well as information such as date of birth, sex, date of validity of an identity document and other data retrieved from the machine readable part of your identity document and/or from the NFC chip of your identity document and/or from the official databases of the competent authorities based in the jurisdiction of the issuing country of your identity document. What data is included at your assignment by Evrotrust in an attributive QCQES will depend on what data you want Evrotrust to certify to the Relying Parties before which you will use such attributive QCQES.

According to the applicable legislation, each qualified trust service provider shall keep a repository of the qualified certificates for electronic signature (hereinafter, **QCESs**) issued by it, as well as of all suspended and terminated QCQESs. This is required in order to enable all Relying Parties to verify the validity of the certificates. Evrotrust maintains a functionality for verification of the validity of the QCESs issued by it.

### **3.3. Data processed in connection with the service for management of remote electronic signature/ seal signature creation devices**

In relation to the provision of the service for management of remote electronic signature/ seal signature creation devices, Evrotrust stores information in the form of logs of the fact and time of the signing , as well as of the fact and time of the sending and receiving of signed documents, together with system identification numbers of the Subscriber and the Relying Party (i.e. the

sender of a document to be signed/ sealed , respectively the recipient of the signed/ sealed document).

### **3.4. Data processed in connection with the issuance of a qualified certificate for electronic seal**

When issuing a qualified certificate for electronic seal, Evrotrust processes the personal data required for identification for the purpose of requesting a service from Evrotrust and entering into a contract with us, described in item 3.1 above.

The content of the certificate for electronic seal issued by Evrotrust is in accordance with the applicable European standards. A certificate issued by Evrotrust will contain the name and, if applicable, the registration number of the seal creator according to the official registers, data for validation of the electronic seal which correspond to the data for creation of the electronic seal, information on the start and end dates of validity of the certificate, information on the issuer, as well as data for the purposes of recognition and verification of the validity of the certificate by the Relying Parties.

### **3.5. Data processed in connection with the issuance of a qualified certificate for website authentication**

When issuing a qualified certificate for website authentication, Evrotrust processes the personal data required for identification for the purpose of requesting a service from Evrotrust services and entering into a contract with us, described in item 3.1.

The content of the qualified certificate for website authentication issued by Evrotrust is in accordance with the applicable European standards. A certificate issued by Evrotrust will contain the name or nickname (in case of a nickname, this is clearly indicated), name of the person to whom the certificate is issued and, if applicable, the registration number, according to the official registers, of the person to whom the certificate is issued (if a legal entity), address details, including, as a minimum, the city/town and country of the person to whom the certificate is issued, the domain name or domain names maintained by the person to whom the certificate is issued, information on the start and end dates of validity of the certificate, information on the issuer, as well as data for the purposes of recognition and verification of the validity of the certificate by the Relying Parties.

### **3.6. Data processed in connection with the creation of a qualified electronic time stamp**

The qualified electronic time stamp relies on the presumption of accuracy of the date and time indicated by it and of the integrity of the data submitted to Evrotrust. The data may be an electronic signature, an electronic seal, a hash of unsigned electronic documents or a hash of other electronic content. A qualified electronic time stamp can be integrated in the process of creating, sending or receiving electronic signatures/seals, electronically signed documents and electronic transactions, in archiving electronic data, etc. This service uses technology to link the date and time to the data in a way that excludes the possibility of any unnoticed change in the data and provides the opportunity to prove in a subsequent period in time (after the expiration of the validity period of the qualified electronic time stamp) the fact of signing of an electronic document or another electronic object.

### **3.7. Data processed in connection with qualified validation of qualified or advanced electronic signature/seal**

When providing the service for qualified validation of qualified or advanced electronic signature/seal, Evrotrust processes the signature/seal validation data contained in the certificate for the qualified or advanced electronic signature/seal, data of the Signatory of the electronic signature/ the Creator of the electronic seal, and other data included in the relevant certificate, the data additionally provided by the Relying Party using the service, as well as the result of the validation performed.

### **3.8. Data processed in connection with the signing of documents through the Application and with the electronic registered delivery service and the service for safe storage (with depository) of documents**

**3.8.1.** Each signing of documents through the Application includes, as integrated services, the service of electronic registered delivery services and safe storage of documents. Therefore, Evrotrust keeps all documents sent by or to you for signing through the functionality of the Application, all documents signed and sent by or to you and information regarding the time of signing, the time of sending and receiving of the documents, Your identification data, sender/recipient identification data, as well as hash value retrieved from the content of the document (metadata). Upon confirmation of the sending, receipt and signing of documents, Evrotrust provides to the sender the hash value as proof with information on the time of sending, receipt and/or signing, information regarding the sender and receiver, information describing

the type of document (document metadata) and stores this information for the period indicated in this Privacy policy, regardless of the erasure of the respective documents.

In relation to the safe storage of documents (with a depository) service - you may at any time access through the Application the electronic documents signed by You. The signed documents may be stored by Evrotrust in an encrypted form for the period agreed between You and Evrotrust. You may request at any time from Evrotrust to delete these documents or use the available functionality for that in the Application (if available). This does not delete the information listed above which has the purpose of evidencing the sending, receiving and signing of documents through the Application.

**3.8.2.** When using the electronic registered delivery service, outside the Applications, Evrotrust keeps information about all documents sent by or to you in the form of electronic acknowledgement receipts / evidence regarding the facts of sending and receiving the documents and the integrity of the transmitted content. Such evidence includes information about the time of sending and receiving the documents, your identification data, the identification data of the sender/recipient, as well as the hash value retrieved from the content of the document (metadata). Upon confirmation of the sending, receipt and signing of documents, Evrotrust provides the sender, as evidence, with an electronic acknowledgement receipt signed by it/ evidence containing information about the time of sending, receiving and/or signing, information about the sender and recipient with a description of the document type (document metadata) and stores such information for the period indicated in this Privacy policy, regardless of the deletion of the documents themselves.

**3.9. Data processed in connection with the provision of the qualified electronic signature/seal and/or electronically signed/sealed electronic documents qualified storage service**

When providing these services, Evrotrust ensures long-term storage of any type of electronic signatures and seals affixed to documents (with temporary storing the documents themselves in a repository) and/or electronically signed/sealed documents (with a repository) for Subscribers of the service and provides evidence of the storage process, with the option to validate the electronic signatures/seals in the long run. The provision of such services requires the storage of the data contained in the relevant electronic signatures and seals and/or in the documents stored. Data objects, the relevant storage evidence and additional information required for their

validation can be accessed by using the service interface or by making a specific request for the provision of data and/or evidence. These may be provided either separately or in an I/O package that is securely protected by encryption. In any case, they are only transmitted to the Subscriber or to their authorized representative. In addition, Evrotrust keeps information on all prepared I/O packages, including the date of the event and the criterion whereby the stored objects included in the package have been selected.

The request must indicate the person requesting the data, the reasons for requesting it, as well as the manner in which it wishes to receive it, and such information is stored by Evrotrust too. At the end of the storage period agreed with the Subscriber, the data will be deleted.

### **3.10. Data processed in connection with the electronic identification service (e-identification/ eID)**

The e-identification service allows you to identify yourself to third parties – Relying Parties, when concluding a contract with such third parties – Relying Parties, using their services remotely, etc. In these cases, the Relying Party sends your personal data (e.g. mobile phone number, e-mail address, etc.) to Evrotrust with a request for you to be identified.

You receive a notification for each request of a Relying Party which wishes you to be identified to it, and information about what data the Relying Party requires from you for this purpose. Such data may be your name, national identification number, image/copy of your identity document and others necessary for your identification to the Relying Party. In order to use the e-identification service, you must carefully review the personal data requested from you and confirm that you wish to be identified with said data to the specified Relying Party. As a result, an electronic document – a statement which contains the specified data about your identity is generated and Evrotrust issues you a short-term attributive QCQES with the content requested by the Relying Party, which is used once, only for identification purposes. If you agree to identify yourself to the Relying Party with the data specified in this document, you sign the latter with the short-term attributive QCQES issued to you for this purpose and instruct Evrotrust to send the signed document – statement to the Relying Party.

### **3.11. Data processed in connection with the electronic identification service through a web interface (WebID)**

The WebID service allows you to identify yourself before third parties – Relying Parties, when concluding a contract, using remote services of the Relying Party, etc., by providing the relevant Relying Party with your personal data necessary for your identification by that Party.

After receiving your request to use the service and your consent with the documents applicable to it, Evrotrust generates an electronic document (file) with structured content in a standardized machine-readable form, which contains information about your identity, extracted from an identity document presented by you and verified with the applicable legally permissible means in accordance with Regulation (EU) No 910/2014. The document is sent to the relevant Relying Party to which you wish to identify yourself.

The document includes at least your names, date of birth, national unique identification number, if any, in accordance with the technical specifications for the purposes of the cross-border identification, which remains unchanged for as long as possible (for example the unified citizen number (EGN) in Bulgaria), identity document number, an image/ copy of your identity document and an image of your signature (specimen) from the presented identity document. Depending on your nationality and the characteristics of the identity document you present, the file may also contain additional specific data, such as: first name (or names) and surname (or names) at birth, place of birth, permanent address, gender, date of issue of identity document and date of expiry of identity document, issuing authority of the identity document, etc.

### **3.12. Data processed in connection with the electronic authentication service**

The electronic authentication service enables you to securely identify yourself when accessing your accounts on various websites and in third-party online services without entering usernames and passwords or as a second step in a secure two-factor identification. When providing this service, information is processed about the website/service which is requested to be accessed, the time at which it is requested to be accessed and whether you have confirmed or refused through the Application that you are the person who requested access to the website or the service.

When providing this service, Evrotrust, on assignment by the Subscriber, generates a document with structured content which contains personal data of the Subscriber in the volume required for their identification to a specific Relying Party for the needs of access to certain content provided

by the latter. As part of the service, the generated document is sent to the Relying Party by Evrotrust without being signed.

### **3.13. Data processed in connection with the use of the Basic Signature service**

When providing the Basic Signature service, Evrotrust stores the received data of the signatory – two names and an e-mail address, and processes the corresponding signature image, as well as metadata related to its use (e.g. date and time of receipt, date and time of signing, system information about the status of the document, etc.)

### **3.14. Data processed in connection with payment for the services**

For the purposes of determining the remunerations due and of processing payments for the provided services, 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 relevant service has been used (in the cases where the services are paid by the Relying Parties).

In case you make payments to us for the use of the services, we will additionally process the following information related to you: VAT number (for natural persons having VAT numbers), BULSTAT (for natural persons having BULSTATs) or other national identification number, payment method, including account from which the payment was made, information about the payments due and made by you, and other data contained in the financial and accounting documents in accordance with the applicable legislation.

### **3.15. Data processed in connection with customer service and in other types of communication with you**

In the performance of customer service, as well as in relation to other types of communication which you address to us, we may process the following personal data:

- e-mail address or telephone number, depending on the channel you have selected for contacting us;
- data regarding your use of the services, as well as other data and information contained in or provided by you within your communication with us and subsequent correspondence;
- data on the time of receiving / sending your message, as well as information on the status of the messages sent by you.



### **3.16. Other information we collect**

**3.16.1.** 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 your 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).

**3.16.2.** Evrotrust keeps records/logs, as provided in the General Terms and Conditions, of all significant events in its systems for a period indicated in this Privacy policy, unless a different period is explicitly provided for in the General Terms and Conditions or in other general terms and conditions applicable to the relevant service, a contract or personal data protection policy.

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

Evrotrust collects, stores and processes the information referred to in item 3 above for the purposes provided for in this Policy and in the General Terms and Conditions. Depending on the legal grounds for the processing, such purposes may be:

- purposes related to compliance with Evrotrust's legal obligations;
- purposes related to and/or necessary for the performance of the contracts entered into between you and Evrotrust, or for taking steps at your request before entering into such contract;
- purposes associated with the legitimate interests of Evrotrust or third parties;
- purposes for which you have consented to the processing of your data.

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

- compliance with the regulatory requirements applicable to the provision of trust services, incl. ensuring your secure identification, verification of the authenticity of the data provided by you, verification of the validity of your identity document, inclusion of the required content in the certificates issued by Evrotrust, etc.;
- compliance with the regulatory requirements for the preservation, publication, provision of or access to information in connection with Evrotrust's activities as a qualified trust service provider;
- fulfillment of Evrotrust's statutory obligations to reproduce and evidence the electronic statements made by you;

- compliance with the applicable tax and accounting legislation;
- other activities associated with fulfilling Evrotrust's legal obligations related to the provision of information to competent governmental and judicial authorities or the provision of assistance in inspections by competent authorities or mandatory inspections related to Evrotrust's regulated activities as a trust service provider.

For the above purposes, we may process all categories of personal data described in item 3 above.

**4.2. The purposes for the processing of personal data by Evrotrust related to and/or necessary for the performance of the contract or for taking steps at the Subscriber's request before entering into a contract with Evrotrust include:**

- activities associated with your identification and/or registration;
- service provision activities;
- communicating with you about the services provided, incl. providing technical support and customer service;
- financial and accounting activities and administration, processing and collection of payments in connection with the services;

For the above purposes, we may process all categories of personal data described in item 3 above.

**4.3. The purposes for the processing of personal data related to the legitimate interests of Evrotrust or third parties include:**

**4.3.1.** Legitimate interest – conclusion, performance, amendment or termination of a contract with a Subscriber, in the cases where the Subscriber is a legal entity and/or acts through its attorney/legal representative as well as where the Subscriber has designated a contact person. The purposes related to the realization of such legitimate interest include all activities referred to in item 4.2 above.

**4.3.2.** Legitimate interest - exercise and protection of Evrotrust's legal rights and interests; and assistance in exercising and protecting the legal rights and interests of Subscribers; of other persons associated with Evrotrust; of the Relying Parties; of Evrotrust employees; of persons processing personal data on behalf of Evrotrust; and of Evrotrust's commercial partners, including:

- establishing, exercising or defending legal claims by the above-mentioned persons, incl. in court, including filing complaints, alerts, etc. with the competent governmental and judicial authorities, responding to legal requests of such authorities, incl. reproducing the retained information within such scope as required to fulfill the purposes;
- taking actions to suspend the provision of services in case of violation of the General Terms and Conditions, or in case of non-compliance with this Policy and the Evrotrust Policies and Practices;
- reproduction of information in connection with the e-identification performed at the request of, and in order to protect the rights and legitimate interests of, the Relying Party;
- reproduction of information in connection with the use of electronic registered delivery at the request of, and in order to protect the rights and legitimate interests of, the sender/recipient;
- administering and servicing of received complaints, alerts, requests, etc., and processing correspondence addressed to Evrotrust, including carrying out checks, collecting additional information and carrying out subsequent communication;
- collection of receivables due to Evrotrust, including through assignment to third parties, as well as transfer of such receivables to third parties (cession).

**4.3.3.** Legitimate interest – provision of the services and their normal functioning:

- maintenance and administration of services;
- taking measures against malicious actions against the security and normal functioning of the services;
- detection and resolution of technical issues related to the functionality of the services;
- creation of a secure environment for the exchange of messages between the Subscriber, Evrotrust and the Relying Party.

**4.3.4.** Legitimate interest – communication and data exchange between companies in the Evrotrust corporate group for the purpose of:

- centralized administrative, financial and accounting servicing;
- execution and servicing of contracts with Subscribers and partners;
- compliance with legal obligations and requirements, including those related to reporting, auditing, carrying out regulated activities, etc.;

- ensuring information security and data security, including sharing indicators of fraud, violations or threats, to protect information systems, databases and equipment, as well as Subscribers, partners and commercial clients;
- establishing, exercising or protecting legal rights and interests of each of the Evrotrust companies;
- providing a data protection officer acting for the Evrotrust group of companies.

For the above purposes, we may process all categories of personal data described in item 3 above.

#### **4.4. Explicit consent**

Your data may be processed on the basis of your explicit consent, the processing in this case being specific and to such extent and within such scope as provided for in the relevant consent.

### **5. WITH WHOM DO WE SHARE YOUR PERSONAL DATA?**

#### **5.1. Data exchange between companies in the Evrotrust group**

When providing the services, the companies in the Evrotrust group, more specifically Evrotrust Technologies AD and its subsidiaries, may exchange personal data with each other in accordance with the intra-group agreement for the exchange of personal data concluded between them and in compliance with all applicable legal and regulatory requirements.

#### **5.2. Provision of data to third parties**

Evrotrust may provide your personal data to third parties only as provided in this Policy, the General Terms and Conditions, other terms and conditions and Policies applicable to the services you use and in the cases provided by law.

Evrotrust may disclose your personal data to third parties:

##### **5.2.1. If this is necessary to fulfill an Evrotrust's legal obligation, for example in the case of an obligation to provide information to:**

- competent governmental, municipal or judicial authorities;
- verification (auditing) authorities.

##### **5.2.2. If this is necessary for the provision of our services, for example when we provide data to:**

- banks and payment service providers in connection with payments made;
- Relying Parties;

- persons to whom you send documents for signing or signed documents by using our services;
- postal and telecommunication operators in the performance of the communication with you.

**5.2.3. if this is this is necessary to protect the rights or legitimate interests of Evrotrust, yourself, or third parties (i.e. our partners, clients or the public interest). In such cases, we may provide your personal data to:**

- governmental, municipal and judicial authorities;
- private and public bailiffs;
- lawyers;
- notaries;
- auditors and other service providers bound by confidentiality obligations.

**5.2.4. If this is necessary in the context of our relationships with parties acting as personal data processors on behalf of Evrotrust, such as a cloud service provider, Evrotrust Registration Authorities (where such activities have been assigned to an external party and it has the role of a data processor), accounting service providers, etc.**

Evrotrust uses partners, subcontractors and service providers, which may process personal information about you on our behalf. Such parties include specialized data centers for reliable and secure colocation of server and network equipment, providers of cloud systems and services, providers of automated identification services, other IT services, etc.

In its work with subcontractors and suppliers, Evrotrust requires them to strictly follow the instructions we provide with respect to personal data processing, in accordance with this Policy.

**5.2.5. In cases where you have given your explicit consent to this.**

**5.2.6. In other cases provided by law.**

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

Evrotrust processes personal data concerning you on the territory of EU/EEA and will not transmit such data to countries outside the EU/EEA. In the event that the provision of certain services involves the transfer of personal data outside the EU/EEA, an adequate instrument is applied between Evrotrust and the relevant person established outside the EU/EEA to ensure data

security (in particular, the European Commission's standard contractual clauses pursuant to Commission Implementing Decision (EU) No 2021/914 of 4 June 2021).

## 7. FOR HOW LONG DO WE STORE YOUR PERSONAL DATA?

**7.1.** Evrotrust processes and stores information about you until the relevant purposes for which it was collected and processed are fulfilled.

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

| Types of data                                                                                                                                                                                                                                                                                                                                                                    | Retention period                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Information about and/or contained in a certificate issued, suspended and terminated by Evrotrust                                                                                                                                                                                                                                                                                | For the entire validity period of the certificate and for a period of 10 (ten) years after its termination                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Information collected and stored in connection with the conclusion and performance of contracts and the provision of trust services, including:                                                                                                                                                                                                                                  | All information collected and stored in connection with the provision of trust services will be retained for the entire period of provision of the relevant service and for a period of 10 (ten) years after its termination, incl. after Evrotrust ceased its activities.<br><br>Such information is stored in order to fulfill Evrotrust's legal obligations under Art. 24 (2)(h) of Regulation (EU) No. 910/2014 and the standards applicable to its activities, and with a view to providing evidence in legal proceedings and ensuring continuity in the provision of the service. |
| <ul style="list-style-type: none"> <li>All information relevant to and all data created or received by Evrotrust in connection with the Subscriber identification and registration process and/or the conclusion of a contract and the performance of such contract (including evidence of the conclusion thereof and acceptance of the General Terms and Conditions)</li> </ul> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <ul style="list-style-type: none"> <li>Information created or received by Evrotrust in connection with the process of providing validation services, electronic qualified delivery, qualified storage of signature/seal, electronic identification and</li> </ul>                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

|                                                                                                                                                                            |                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| electronic authentication, including logs for all events related to the issuance, effect and validity of the keys, incl. information about each generated key pair         |                                                                                                                                                                                       |
| <ul style="list-style-type: none"> <li>Information contained in the communication with Subscribers in connection with the services</li> </ul>                              |                                                                                                                                                                                       |
| Information related to the use of the service for qualified storage of electronically signed documents (with a repository): documents sent for signing or signed documents | Until their deletion by the Subscriber or until the termination of its contract, but not more than ten (10) years                                                                     |
| Statements electronically signed with an attributive QCQES, which contain information about your identity (for the electronic identification service)                      | Up to two (2) hours from the signing thereof                                                                                                                                          |
| Information related to the use of the service for storage of qualified electronic signatures: your private keys in encrypted form                                          | For the validity period of the QCQES issued                                                                                                                                           |
| Information related to the use of the electronic authentication service                                                                                                    | Up to one (1) year from the performance of the relevant action                                                                                                                        |
| Information related to the use of the Basic Signature service                                                                                                              | Up to ten (10) years                                                                                                                                                                  |
| Financial and accounting documents; invoices; other information related to tax and social security control.                                                                | Up to ten (10) years, from the beginning of the year following the year during which the payment of the liability for the relevant year is due                                        |
| System logs. Security-related logs, etc. (may contain information such as: date and time, IP address, URL, browser version and device information)                         | Up to one (1) year from the generation of the relevant log, unless a different period has been provided for in this Policy, in the General Terms and Conditions or in other terms and |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | conditions or Policy applicable to the relevant service                                                                                                                                                                                                                                                     |
| Data and records collected in case of failed identification                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Two (2) months from its implementation                                                                                                                                                                                                                                                                      |
| Data contained in and processed in connection with correspondence addressed to Evrotrust, as well as in relation to customer service, collection of additional information, and carrying out subsequent communication in connection with the received correspondence                                                                                                                                                                                                                                                                                                                                                                                       | When there is no statutory retention period or one is not defined above in this Policy, 5 (five) years from the last communication and related relationships                                                                                                                                                |
| Data processed in accordance with a personal data protection policy applicable to the use of specific services (e.g. personal data protection policy applicable to the use of an Evrotrust Application)                                                                                                                                                                                                                                                                                                                                                                                                                                                    | In accordance with the periods provided for in the relevant personal data protection policy. In case the relevant personal data protection policy does not stipulate any specific periods for the processing and storage of personal data - then the periods referred to in this Policy shall be applicable |
| Data processed on the basis of your explicit consent                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | From the time of giving the consent until its withdrawal by the data subject, unless a shorter period has been provided for in the specific consent or in additionally applicable Personal Data Protection Policies                                                                                         |
| <p>In case of a legal dispute or proceedings requiring data retention and/or at the request of a competent governmental authority, it is possible to retain data for longer than the above stated periods until the final resolution of the dispute or completion of the proceedings before all instances, as well as for up to five (5) years after the final resolution of the relevant dispute or completion of the relevant proceedings.</p> <p>The personal data referred to in this Policy may be processed for longer than the above stated periods, if this is necessary to fulfill the purposes provided for therein or to protect the rights</p> |                                                                                                                                                                                                                                                                                                             |



and/or legitimate interests (including in court) of Evrotrust or third parties, or if the applicable legislation provides for the processing of such 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. Right to information**

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 the subject of a decision solely based on automated processing, including profiling, which has legal consequences for you or similarly affects you significantly, unless the grounds for this as provided for in the applicable personal data protection legislation exist and appropriate warranties have been provided to protect your rights, freedoms and legitimate interests.

#### **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.

#### **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**

You may exercise the rights described above at any time by sending a written request to the Evrotrust DPO - by post to the contact address or by e-mail to the e-mail address referred to in item 9 of this Policy, as provided for in the applicable legislation.

#### **8.12. Right to lodge a complaint with a supervisory authority**

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

The supervisory authority in the Republic of Bulgaria is the Commission for Personal Data Protection, address: 2 Prof. Tsvetan Lazarov Blvd., 1592 Sofia, Bulgaria, website: <https://www.cpdp.bg/>.

You can find information about the supervisory authorities of other Member States [here](#).

### **8.13. Rights of data subjects outside the EU/EEA**

Evrotrust respects, and nothing in this Policy is intended to limit, the rights granted to you by applicable to you mandatory rules of a national law of a country outside the EU/EEA, including your right to lodge a complaint with a relevant authority provided for in the legislation applicable to you.

## **9. WHO CAN YOU CONTACT IN RELATION TO THE PROCESSING OF YOUR PERSONAL DATA AND THE EXERCISE OF YOUR RIGHTS? OUR DATA PROTECTION OFFICER (DPO)**

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:

tel.: +359 2 448 58 58

e-mail address: [dpo@evrotrust.com](mailto:dpo@evrotrust.com)

address: 251G Okolovrasten pat Str., MM Business Center, floor 5, 1766 Sofia, Bulgaria

## **10. SPECIAL RULES**

### **10.1. SPECIAL RULES REGARDING NORTH MACEDONIA**

*The rules in this section apply only with respect to the territory of North Macedonia, and are applied in addition to the other rules described in this Policy, taking precedence over them in case of conflict or discrepancies.*

**10.1.1.** On the territory of North Macedonia the services described in the General Terms and Conditions and this Policy are provided by Evrotrust Technologies DOOEL – Skopje, a limited liability company, with a single tax number (UTN) 4080020591119, address: 1/2-31 Veniamin Machukovski Str., fl. 3, 1000 Skopje, North Macedonia (hereinafter, **Evrotrust Macedonia**), tel.: +389 2 3109 300, +389 2 314 4444, website: <http://evrotrust.mk/en/>, e-mail: [office@evrotrust.mk](mailto:office@evrotrust.mk), [support@evrotrust.mk](mailto:support@evrotrust.mk).

**10.1.2.** Evrotrust Macedonia is the data controller of the personal data processed in connection with the provision of the services and performs this activity in full accordance with what is described in this Policy regarding these services, as well as in accordance with the legal

requirements and rules applicable on the territory of the Republic of North Macedonia for the protection of personal data.

**10.1.3.** All references to Evrotrust contained in this Policy should be understood as references to Evrotrust Macedonia, insofar as the relevant texts relate to the provision of the services on the territory of the Republic of North Macedonia, including as regards the Data Subjects whose data is processed in relation to the provision of the services, and who have all rights described in this Policy, towards Evrotrust Macedonia.

**10.1.4.** The supervisory authority for the protection of personal data in the Republic of North Macedonia is the Personal Data Protection Agency of the Republic of North Macedonia, with address: 18 Gotse Delchev Blvd., Skopje, Republic of North Macedonia, website: <https://azlp.mk>.

**10.1.5.** You can address all your requests and questions related to the protection of your personal data and the exercise of your rights according to the legislation on the protection of personal data, in connection with the provision of the services on the territory of the Republic of North Macedonia, to the DPO of Evrotrust Macedonia at e-mail address: [dpo@evrotrust.com](mailto:dpo@evrotrust.com), tel.: +359 2 448 58 58, address: 251G Okolovrasten pat Str., MM Business Center, 5th floor, 1766 Sofia, Bulgaria.

## **10.2. SPECIAL RULES REGARDING ROMANIA**

*The rules in this section apply only with respect to the territory of Romania, and are applied in addition to the other rules described in this Policy, taking precedence over them in case of conflict or discrepancies.*

**10.2.1.** On the territory of Romania, the electronic identification – eID, and electronic identification via web interface – webID services, described in items 3.10 and 3.11 of this Policy, are provided by Evrotrust Technologies SRL, a limited liability company, with registration number 49798208, address: Strada Nerva Traian, Nr. 27-33, Birou Nr. 6, Scara B, Etaj 1, București Sectorul 3, Romania (hereinafter, **Evrotrust Romania**), tel.: +359 2 448 58 58, e-mail address: [office@evrotrust.com](mailto:office@evrotrust.com), [support@evrotrust.com](mailto:support@evrotrust.com).

**10.2.2.** Evrotrust Romania is the data controller for the personal data processed in connection with the provision of the services specified under item 10.2.1 above and carries out this activity fully in accordance with this Policy with respect to those services, as well as in accordance with the applicable legal requirements and data protection rules in Romania.

**10.2.3.** When using the services under item 10.2.1 above, under the applicable Romanian

legislation you need to expressly confirm your consent to the identification process and the purposes of the identification described in this Policy. You need to also provide your explicit consent for the capturing and/or recording of your image, as well as the image of your identity document. Evrotrust Romania collects your consent in the manner described in the relevant consent declaration and in compliance with all applicable legal requirements.

**10.2.4.** All references to Evrotrust contained in this Policy shall be understood as references to Evrotrust Romania, insofar as the relevant provisions relate to the provision of the services under item 10.2.1 above on the territory of Romania, including with respect to Data Subjects whose personal data are processed in relation to those services and who have all the rights described in this Policy towards Evrotrust Romania.

**10.2.5.** The supervisory authority for data protection in Romania is the National Supervisory Authority for Personal Data Processing (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal), address: B-dul G-ral. Gheorghe Magheru 28-30 Sector 1, P.O. Box 010336, Bucharest, Romania, website: <https://www.dataprotection.ro/>.

**10.2.6.** You may address all your requests and questions related to the protection of your personal data and the exercise of your rights under data protection legislation, in connection with the provision of the eID and webID services on the territory of Romania, to the DPO of Evrotrust Romania, at: [dpo@evrotrust.com](mailto:dpo@evrotrust.com), tel.: +359 2 448 58 58, address: 251G Okolovrasten Pat Str., MM Business Center, 5th floor, 1766 Sofia, Bulgaria.

### **10.3. SPECIAL RULES REGARDING KENYA**

*The rules in this section apply only with respect to the territory of Kenya and to citizens of Kenya, and are applied in addition to the other rules described in this Policy, taking precedence over them in case of conflict or discrepancies.*

**10.3.1.** If you are a citizen of Kenya, the processing of your personal data is carried out by Evrotrust Technologies AD in accordance with this Policy and in strict compliance with the applicable legal requirements and data protection rules in Kenya and with respect to Kenyan citizens.

**10.3.2.** The supervisory authority for data protection in Kenya is the Office of the Data Protection Commissioner, address: Britam Tower, 12th & 13th floor, Hospital Road, Upper Hill – Nairobi, email: [info@odpc.go.ke](mailto:info@odpc.go.ke), website: <https://www.odpc.go.ke/>.

**10.3.3.** Evrotrust Technologies AD is registered with the Office of the Data Protection

Commissioner as a data controller under number 3415. You may address all your requests and questions related to the protection of your personal data and the exercise of your rights under Kenyan data protection legislation to the DPO of Evrotrust at: [dpo@evrotrust.com](mailto:dpo@evrotrust.com), tel.: +359 2 448 58 58, address: 251G Okolovrasten pat Str., MM Business Center, 5th floor, 1766 Sofia, Bulgaria.

## **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](http://www.evrotrust.com) and <http://evrotrust.mk/en/>.

*This document is published in Bulgarian, English or another language. In case of discrepancy between the Bulgarian and English texts, the Bulgarian text takes precedence. In case of inconsistency between the English and other language texts, the English text shall prevail.*