ISO 9001:2015 ISO 27001:2013
ISO 20000-1:2018 ISO 22301:2019
Regulation (EU) 910/2014
Regulation (EU) 2016/679

GENERAL TERMS AND CONDITIONS OF THE CONTRACT FOR TRUST, INFORMATION, CRYPTOGRAPHIC AND OTHER SERVICES

CONTENTS

1 OVERVIEW

1.1 INFORMATION ABOUT EVROTRUST TECHNOLOGIES AD

Evrotrust is a qualified provider of trust carrying out its activities in accordance with the requirements of Regulation (EU) № 910/2014 and the Bulgarian Electronic Document and Electronic Trust services Act (EDETSA) and as such it is included in the trusted list of European trust service providers and in the register of the Bulgarian trust service providers kept by the Communications Regulation Commission in the Republic of Bulgaria.

Evrotrust's contact details:

Company name	Evrotrust Technologies AD
UIC	203397356
Seat, registered address and postal address	2 Nikolay Haytov St, entr.D, fl.2, Iztok Res. Complex, Izgrev Region, Sofia 1113
Office address and internal registration authority address	Sofia, 1766 "Okolovrasten pat" 251G, Business center MM, floor 5
Phone	(+359 2) 448 58 58
Fax	(+359 2) 448 58 58
E-mail address	info@evrotrust.com office@evrotrust.com
Web page/ website	https://www.evrotrust.com/

1.2 SUBSCRIBERS SERVICE

Evrotrust provides qualified and unqualified trust services through a Certification Authority and an internal Registering Authority as well as through a network of external Registering Authorities. The external Registering Authorities perform their activities for the provision of trust services on behalf of Evrotrust. A full and up-to-date list of the Registering Authorities and information about their contact details are available on Evrotrust's web page: https://www.evrotrust.com/.

1.3 SUPERVISORY AUTHORITY

The Communications Regulation Commission (CRC) is the national supervisory authority in the Republic of Bulgaria exercising the powers under Regulation (EU) № 910/2014 and

EDECSA. On the grounds of Art. 32 of EDECSA, CRC grants qualified status to trust services providers, controls the observation of security requirements and creates, maintains and publishes the national trusted list of persons providing trust services and qualified trust services.

Contact address:

6 Gen. Yosif V. Gurko St, Sofia 1000,

Phone: (+359 2) 949 27 23

Fax: (+359 2) 987 06 95

E-mail: info@crc.bg

Web page: https://crc.bg/bg/

1.4 GENERAL TERMS AND CONDITIONS. ACCESS TO AND PROVISION OF GTC ON A DURABLE MEDIUM

1.4.1. This document constitutes the General Terms and Conditions under which the contracts for using the trust, cryptographic, information and other services provided by Evrotrust Technologies AD (Evrotrust) are concluded (GTC) and forms an integral part of the contracts for using the respective services. This document has an assigned unique object identifier (OID): 1.3.6.1.4.1.47272.3.1.2.

1.4.2. These GTC are applied in the relationship with all Subscribers, namely in the relationship with Signatories, Creators and all other Subscribers who have concluded a contract with Evrotrust for services provided by Evrotrust according to the procedure determined herein. These GTC are also applied with respect to the Relying Parties who rely on electronic identification or on a trust service provided by Evrotrust.

1.4.3. These GTC are publicly available on Evrotrust's web page https://www.evrotrust.com/, in Evrotrust's mobile applications, and in any office of Evrotrust or of an external Registering Authority of Evrotrust. The GTC have been published in Bulgarian and English.

1.4.4. Each Subscriber and each Relying Party undertake to make themselves familiar with these GTC before concluding a contract with Evrotrust and using any of the services subject to

these GTC and, respectively, before trusting and relying as Relying Parties on electronic identification or a trust service provided by Evrotrust.

1.4.5. Depending on the manner in which Evrotrust's services are requested and/or used by the Subscribers and the Relying Parties, GTC are provided and accessible in a suitable way in a readable form and on a durable medium as follows:

(1) When a contract is concluded with Evrotrust in an office of Evrotrust or an office of an external Registering Authority of Evrotrust on paper, GTC are provided to the Client on paper.

(2) When a contract is concluded with Evrotrust in electronic form, through a channel of communication with Evrotrust other than a mobile application, or by appearing in person in an office of Evrotrust or in an office of an external Registering Authority of Evrotrust, GTC are provided to the Subscriber on a durable medium by sending them as an attached and electronically signed file by e-mail to an e-mail address indicated by the Subscriber within the conclusion of the contract. If the Subscriber does not have an e-mail address and insofar as the Policies and Practices applicable to the specific service(s) that are subject to the contract allow the provision of those services without the Subscriber's supplying a valid e-mail address, GTC are sent to the Subscriber through a link in an SMS with the instruction that they should be immediately downloaded by the Subscriber and saved on their local device.

(3) When the contract is concluded through a mobile application of Evrotrust, the GTC signed by the client and Evrotrust are available for downloading in the respective mobile application. In such cases, the Client undertakes to download and store on their local device the documents signed upon the conclusion of the contract under these GTC (GTC, an applicable Personal Data Protection Policy, Declaration of Consent, etc.).

(4) In addition to the foregoing, GTC are available in readable form for a long period of time on Evrotrust's website in a format allowing their downloading, storage and reproduction in electronic form as well as printing them out on paper. Upon request at an office of Evrotrust, they can be provided to the Subscriber in paper form at any time.

2 SERVICES PROVIDED BY EVROTRUST

These GTC are applied in the relationship between Evrotrust and the Subscribers as well

as in the relationship between Evrotrust and the Relying Parities when the trust services described further on in this section are provided.

2.1 ISSUING A QUALIFIED CERTIFICATE FOR ELECTRONIC SIGNATURE

A Qualified Certificate for Electronic Signature in accordance with Art. 28 of Regulation (EU) № 910/2014 is issued only to a natural person (Electronic Signature Signatory/ Signatory). Depending on the profile and its issuance Policy, it may be used to certify authorship on electronic documents, for identification or authentication upon access to web applications, protected communications and electronic signing of all types of documents (PDF (PaDES), XML(XaDES), TXT(CaDES), etc.). Qualified certificates for electronic signature may also be used to sign document packages (ASiC-E), as well as e-mail (based on S/MIME (Secure/ Multipurpose Internet Mail Extensions/ Protocol for secure e-mail transmission via the Internet or a cryptographic system for protecting the messages transmitted via e-mail and the data stored on various media)). The certificate may also include data about a legal entity associated with the natural person on whose behalf the Signatory will sign. In such a case, Evrotrust does not certify the representative power of the natural person Signatory against the legal entity but only that there exists a legal relation of the Signatory to the legal entity.

Types of profiles of qualified certificates for electronic signature issued by Evrotrust:

2.1.1. Evrotrust Qualified Natural Person Certificate for QES, OID: 1.3.6.1.4.1.47272.2.2

The issuance of such a certificate is a qualified trust service pursuant to Regulation (EU) № 910/2014. A Qualified Natural Person Certificate for QES is issued for the purpose of establishing the authorship of a natural person Signatory on electronic documents signed electronically and accompanied by the certificate.

2.1.2. Evrotrust Qualified Natural Person Attribute Certificate for QES, OID: 1.3.6.1.4.1.47272.2.2.1

The issuance of such a certificate is a qualified trust service pursuant to Regulation (EU) № 910/2014. A Qualified Natural Person Attribute Certificate for QES is issued for the purpose of identifying the natural person Signatory with specific additional attributes as described in the

certificate. All procedures and rules for its issuance and management match those of the certificate under item 2.1.1. The difference in the case of this certificate consists in the volume and type of the data certified.

The services under item 2.1.1 and item 2.1.2 are related to using a Qualified (Electronic) Signature Creation Device (QSCD) when creating an electronic signature. The "Qualified Statements" attribute in the certificate contains an instruction that the certificate is qualified and shows whether the private key has been used for creating the electronic signature in a Qualified (Electronic) Signature Creation Device (QSCD/ Secure Signature Creation Device). In this case, Evrotrust issues the certificate and hands it over to the signatory or to a person expressly authorized by the Signatory. By accepting these GTC when requesting this service, it is considered that the Signatory agrees to the use of the Qualified (Electronic) Signature Creation Device.

2.1.3. Evrotrust Qualified Natural Person Certificate for AES, OID: 1.3.6.1.4.1.47272.2.7.

The issuance of such a certificate is a qualified trust service pursuant to Regulation (EU) № 910/2014.

A Qualified Certificate for AES is issued subject to the observation all Policies and Practices for issuing qualified certificates under 2.1.1 and 2.1.2. The difference is that the electronic signature is not created in a Qualified (Electronic) Signature Creation Device.

2.2 REMOTE ELECTRONIC SIGNATURE/SEAL CREATION SERVICE (RESS)

This service allows the remote signing with a qualified and advanced signature or, respectively, the remote creation of a qualified electronic seal. When this service is used, the electronic signature/electronic seal is created with a "remote signature/seal creation device" – the seal creation device is not a personal device physically controlled by the Signatory / Creator but is replaced by services offered and managed by Evrotrust. When this service is used, the Electronic Signature Signatory / the Electronic Seal Creator assigns the servicing of Qualified Electronic Signature/Seal Creation Devices to Evrotrust, and Evrotrust applies mechanisms and procedures meeting the requirements of Regulation (EU) № 910/2014 and guaranteeing that the Signatory/Creator has sole control over the use of the data related to the creation of their electronic signature/seal, and that the requirements regarding the qualified electronic

signature/seal are fulfilled when using the device. Evrotrust provides a service for the remote creation of electronic signatures/seals where it manages the electronic signature/seal creation environment on behalf of the Electronic Signature Signatory / Electronic Seal Creator. To guarantee that the electronic signatures/seals receive the same legal recognition as the electronic signatures/seals created in an environment fully managed by the Signatory /Creator, Evrotrust applies specific procedures concerning the security of management and the administrative security and uses reliable systems and products, including secure electronic communication channels, a reliable electronic signature/seal creation environment, and guarantees that this environment is used only under the control of the Electronic Signature Signatory / Electronic Seal Creator ("sole control").

The Remote Electronic Signature Creation Service is accessible:

1. Through a mobile application of Evrotrust installed on a smart device;
2. When requesting a short-term qualified electronic signature certificate at an office of a Registering Authority. The short-term qualified electronic signature certificate is a Qualified Electronic Signature Qualified Certificate (QESQC) which is issued by Evrotrust to the Signatory for the purpose of a single signing of an electronic document or an electronic document package.

This service is provided pursuant to the requirements of Regulation (EU) № 910/2014 and the applicable standards for remote qualified electronic signature creation in a remote-signing hardware cryptomodule certified by an accredited laboratory and a protected certified environment (Tamper-protected Environment), as well as subject to observing a remote-signing Policy and Practice.

2.3 ISSUING A QUALIFIED CERTIFICATE FOR ELECTRONIC SEAL

A Qualified Certificate for Electronic Seal is issued only to a legal person (Seal Creator/ Creator) and may be used to guarantee the origin and integrity of the legal person's output data, for instance: electronic documents, photographs, architectural projects, software, etc. This trust service of Evrotrust is provided in accordance with Art. 38 of Regulation (EU) № 910/2014.

Types of profiles of Qualified Certificates for Electronic Seal issued by Evrotrust:

2.3.1. Evrotrust Qualified Legal Person/Organization Certificate for QESeal, OID: 1.3.6.1.4.1.47272.2.3 – a qualified trust service;

The issuance of such a certificate is a qualified trust service from Regulation (EU) № 910/2014.

This service is related to the use of a Qualified (Electronic) Signature/Seal Creation Device (QSCD) when creating the electronic seal. The "Qualified Statements" attribute in the certificate contains an instruction that the certificate is qualified and shows whether the private key has been used for creating the electronic seal in a Qualified (Electronic) Signature Creation Device (QSCD/Secure Signature Creation Device). Evrotrust issues the certificate and delivers it to a person empowered by the legal entity Creator.

By accepting these GTC when requesting this service, it is considered that the Creator agrees to use a qualified device for the creation of a qualified electronic signature.

2.3.2. Evrotrust Qualified Legal Person/Organization Certificate for AESeal, OID: 1.3.6.1.4.1.47272.2.8;

The issuance of such a certificate is a qualified trust service from Regulation (EU) № 910/2014. This qualified certificate is issued subject to observing all Policies and Practices for the issuance of a qualified certificate under 2.3.1. The difference is that the electronic seal is not created in a Qualified Electronic Seal Creation Device.

2.3.3. Evrotrust Qualified PSD2 Legal Person/Organization Certificate for AESeal, OID: 1.3.6.1.4.1.47272.2.8.1;

The issuance of such a certificate is a qualified trust service from Regulation (EU) № 910/2014. This certificate is a Qualified Legal Person/Organization Certificate for AESeal, which is intended to be used for fulfilling the requirements of the Payment Service Directive (Directive (EU) № 2015/2366; PSD2).

2.4 ISSUING A QUALIFIED CERTIFICATE FOR WEBSITE AUTHENTICATION

A Qualified Certificate for Website Authentication is issued for the purpose of certifying

the holding of a website by a particular natural person or legal entity. It is intended to be used for creating certainty in a visitor that the website is maintained by a real and identified subject. Using the SSL-technology ensures reliable connectivity under a secure protocol for the exchange of information between the website and its visitors. This qualified trust service is provided by Evrotrust in accordance with Art. 45 of Regulation (EU) № 910/2014.

Types of profiles of Qualified Certificates for Website Authentication issued by Evrotrust:

2.4.1. Evrotrust SSL PSD2 Certificate, OID: 1.3.6.1.4.1.47272.2.5.1

The issuance of such a certificate is a qualified trust service in accordance with Art. 45 of Regulation (EU) № 910/2014. Such a qualified certificate is issued for the purpose of authenticating a website related to a payment service provider under PSD2 and is intended to be used for fulfilling some requirements of PSD2. It has the nature of a qualified website certificate within the meaning of Regulation (EU) № 910/2014 and is used to create certainty in a visitor that the website is maintained by a real and identified subject. Using this technology ensures reliable connectivity under a secure information exchange protocol.

2.4.2. Evrotrust SSL EV Certificate, OID: 1.3.6.1.4.1.47272.2.5

The issuance of such a certificate is a qualified trust service in accordance with Art. 45 of Regulation (EU) № 910/2014. Such a certificate is used to create certainty in a user that the website is maintained by the real and identified subject specified in the certificate. During this certificate issuance an extended validation of the organization holding the website is performed.

2.4.3. Evrotrust SSL Organization Validated, OID: 1.3.6.1.4.1.47272.2.4.2

The issuance of such a certificate is a qualified trust service in accordance with Art. 45 of Regulation (EU) № 910/2014. This certificate attests to the Signatory ship of the website and confirms the existence of the organization shown as the Signatory of the website.

2.4.4. Evrotrust SSL Domain Validated Certificate, OID: 1.3.6.1.4.1.47272.2.4.1

The issuance of such a certificate is a qualified trust service in accordance with Art. 45 of Regulation (EC) № 910/2014. When issuing such a certificate, Evrotrust makes a check as to

whether the registration and ownership of the domain in the public WhoIs databases corresponds to the person that requested it. If such public information is missing, the Client provides information on their own which proves the ownership of the domain and is verified by Evrotrust.

2.5 ISSUING A QUALIFIED ELECTRONIC TIME STAMP

The issuance of a Qualified Electronic Time Stamp, OID: 1.3.6.1.4.1.47272.1.2, is a qualified trust service which Evrotrust provides in accordance with Art. 42 of Regulation (EU) № 910/2014. Qualified Electronic Time Stamps are issued to natural persons and legal entities. A Qualified Electronic Time Stamp enjoys the presumption of accuracy of the date and time that it indicates and of integrity of the data presented before Evrotrust. Such data may be an electronic signature, an electronic seal, a hash of unsigned electronic documents or a hash of some other electronic content.

The Qualified Electronic Time Stamp may be integrated in the process of creating, sending or accepting the electronic signatures/seals, electronically signed documents and electronic transactions, when archiving electronic data, etc. This service uses a technology of binding the date and time to the data in a way that excludes the possibility of an unnoticed change of the data and provides a possibility of proving, in a subsequent period of time (after the expiry of the validity period of the Qualified Electronic Time Stamp), the fact that an electronic document or another electronic item has been signed.

2.5.1 Specific Requirements Applicable to the Relying Parties

The main obligation of the Relying Party is to check the validity of the signature/seal on the electronic time-stamp token (TST). The Relying Party must check the validity of the time stamp (TSU/ Time Stamp Unit) as well as the validity period of this certificate. If any time stamps are checked after the expiry of the validity period of the TSU certificate, the Relying Party must:

(1) check for the time-stamp certificate in the Certificate Revocation List (CRL);

(2) check the applicability of the hash algorithm used;

(3) ascertain the security of the electronic signature used by checking the applicable combination of asymmetric and hash algorithms.

When relying on a Qualified Electronic Time Stamp the Relying Party is obliged to:

(1) verify that the a Qualified Electronic Time-Stamp has been correctly signed and that the

private key used to sign the time-stamp has not been compromised until the time of the verification.

(2) take into account any limitations on the usage of the time-stamp indicated by these Terms and Conditions and in the applicable Policies and Practices; and

(3) take into account any other precautions prescribed in these Terms and Conditions and in the applicable Policies and Practices.

2.6 QUALIFIED VALIDATION SERVICE FOR QUALIFIED ELECTRONIC SIGNATURES/ SEALS

The Qualified Validation of a Qualified Electronic Signature/Seal, OID: 1.3.6.1.4.1.47272.2.9, is a qualified trust service in accordance with Art. 32, 33 and 40 of Regulation (EU) № 910/2014. This service is used to validate electronic signatures, electronic seals, registered e-mail services and certificates related to those services and issued by Evrotrust. Validation is also made of qualified website authentication certificates. The qualified validation service is provided by Evrotrust in its capacity of qualified trust services provider and as a result of its provision a special document certifying the validity is generated and given to the Client.

In the process of validating a qualified electronic signature/seal, Evrotrust confirms the validity of the qualified electronic signature/seal provided that:

1. The certificate that accompanied the signature/seal at the time of signing was a qualified electronic signature/seal certificate meeting the requirements of Regulation (EU) № 910/2014;
2. The qualified certificate was valid at the time of signing.

This service may be provided to validate qualified certificates for electronic signatures, seals and other qualified certificates issued by qualified trust service providers included in the trusted list of the European Commission. These trust services of Evrotrust are provided in accordance with Art. 33 and Art. 40 of Regulation (EU) № 910/2014.

2.6.1. Specific Requirements Applicable to the Qualified Validation of a Qualified Electronic Signature/Seal Service. Accessibility and Level of Service (SLA)

2.6.1.1. The qualified validation service accessible through Evrotrust's web page is intended for private, non-commercial use without any commitment of the part of Evrotrust as to

its level of service. To use the service at the respective level of service or automated, it is necessary to conclude an additional contract under which the services may be provided automated through a relevant interface (API), which also regulates the offered level of service (SLA). All specific conditions, formats and validation service algorithms used are described in the document "Policy and Practice of a Qualified Validation Service for Qualified Electronic Signatures/Seals".

The status for electronic signature/seal validation and the document confirming or not the validity of the electronic signature/seal (report) are related to the conformity Practices, Policies and arrangements of other service providers who are not controlled by Evrotrust. In this case there may be a delay in providing information about a certificate revocation status and a Client/Relying Party may have to wait for the publishing of the respective Certificate Revocation List (CRL) by the respective provider and even for one more subsequent update of CRL to guarantee that each respective revocation request has been processed.

2.6.1.2. The service supports the following options:

(1) The service allows the Client to choose the Signed Data Object (SDO) and the Signer's Document (SD);

(2) The service may allow the user to provide additional data about the validation process: (a) the certificates that must be used for validation, e.g. the case when the SDO attributes do not contain the required certificates; (b) the specific signature that must be checked in case SDO contains multiple signatures, and (c) the policy to be used for the implicit or explicit validation of the signature.

2.6.1.3. Evrotrust supports signature formats determined in ETSI EN 319 122 - 1 and ETSI EN 319 122 - 2 or in ETSI EN 319 132 - 1 and ETSI EN 319 132 - 2 or in ETSI EN 319 142 - 1 and ETSI EN 319 142 - 2.

2.6.1.4. Supported formats with basic electronic signature/seal profile:

(1) ETSI TS 103 171 Electronic Signatures and Infrastructures (ESI) - XadES Baseline Profile;

(2) ETSI TS 103 173 Electronic Signatures and Infrastructures (ESI) - CadES Baseline Profile;

(3) ETSI TS 103 172 Electronic Signatures and Infrastructures (ESI) – PadES Baseline Profile;

(4) ETSI TS 103 174 Electronic Signatures and Infrastructures (ESI) – AsiC Baseline Profile

Additionally, Evrotrust validates the above formats but with an extended profile and levels:

(1) ETSI TS 103 171 Electronic Signatures and Infrastructures (ESI) – XadES -T/TL Level;

(2) ETSI TS 103 173 Electronic Signatures and Infrastructures (ESI) – CadES T/TL Level;

(3) ETSI TS 103 172 Electronic Signatures and Infrastructures (ESI) PadES T/TL Level;

(4) ETSI TS 103 174 Electronic Signatures and Infrastructures (ESI) AsiC T/TL Level.

2.6.1.5. Evrotrust's validation service validates the following electronic signature/seal type formats:

(1) Attached - Enveloping – the electronic signature/seal envelops the signed item;

(2) Attached - Enveloped – the signed item envelops the electronic signature/seal;

(3) Detached – the electronic signature is outside the signed item – in a separate file/item; and

(4) One document signed electronically with more than one electronic signature/seal.

2.6.1.6. The service successfully validates electronic signatures/seals with expired or outdated elements such as certificates with an expired validity period or time-stamps, coordinating the check with the certified date and time when the electronic signature/seal was affixed. If no such time has been certified, the check is made as at the present time and if the validity of the elements has expired, this makes it impossible to confirm the validity of the signature/seal, which is noted down in the validity report. When revoked certificates have been used, the service checks whether they were valid at the time of signing and, if not, the service notes down in the validity report that it is impossible to validate the signature. If an algorithm has been used outside its applicable period, the service notes down an electronic signature in the

report as invalid for this reason.

2.6.1.7. Evrotrust chooses the validation limitations when the Client provides a conflicting indication which contradicts Evrotrust's practice. Evrotrust does not allow the Client to set the a custom signature verification policy.

2.6.1.8. In its applicable Policies and Practices, Evrotrust indicates how it acts when it is impossible to process the limitations submitted by the Client, under what conditions the Signature Verification Policy may be ignored and replaced with rules for validating the signature in accordance with the protocol specified in ETSI TS 119 442, which supports various options and specifies what is considered proof of existence (PoE) of a signature.

2.7 QUALIFIED REGISTERED E-MAIL

The Qualified Registered E-Mail is a trust service allowing the transmission of data between third parties electronically and provides evidence with respect to the identity of the sender and the recipient of the transmitted data, the time of sending and receiving the data and protects the transmitted data against the risk of loss, theft, damage or unauthorized changes.

The service provides:

(1) a high level of trust as regards the sender's identification;

(2) the sender's identification before the delivery of the data;

(3) The sending and receiving of data is secured through an advanced electronic signature or an advanced electronic seal of Evrotrust in a way excluding all possibilities for unnoticed change of the data;

(4) Each data change necessary for the purpose of sending or receiving the data is clearly marked for the sender and for the recipient of the data;

(5) The date and time of sending and receiving as well as any change of the data are indicated by a Qualified Electronic Time-Stamp.

When providing this service, Evrotrust creates, signs with an advanced electronic seal and gives to the sender proof (electronic advice of delivery) regarding the facts of the sending,

receiving and integrity of the content transmitted.

This trust service of Evrotrust is provided in accordance with Art. 44 of Regulation (EU) № 910/2014.

The proof of the messages transmitted may be stored for a period of 10 years in Evrotrust's repository. It may be provided to the parties in accordance with the applicable prices and conditions.

Types of electronic registered delivery services provided by Evrotrust:

2.7.1. Qualified electronic registered delivery service (QERDS), OID: 1.3.6.1.4.1.47272.2.10.1

This service is provided by Evrotrust in accordance with Art. 44 of Regulation (EU) № 910/2014 and relies on technology that enables the delivery of electronic registered mail from a mobile application to a mobile application, from a mobile application to an API and back, and from a mobile application to a web page on a specialized portal and back.

2.7.2. Qualified electronic registered delivery service (REM), OID: 1.3.6.1.4.1.47272.2.10.2 - qualified trust services:

This service is provided by Evrotrust in accordance with Art. 44 of Regulation (EU) № 910/2014 and relies on technology that enables the delivery of electronic registered mail via a specialized electronic mail server (SMTP) and is accessible through standard mail clients such as Mozilla Thunderbird , etc., as well as through the web based e-mail application.

2.7.3. Specific requirements for the provision of a qualified electronic registered delivery service

2.7.3.1. Successful delivery of electronic content

(1) A successful delivery shall be considered to have taken place where the content sent by the sender has left the information system of the sender and is no longer under its control.

(2) A delivery shall be considered to have been served where the content sent by the sender has successfully entered the information system of the recipient.

(3) When using an mobile application of Evrotrust, successful content sending shall be considered the receipt of the electronic message on the Evrotrust backend (server), and successful content delivery shall be considered the receipt of the sent electronic content in the mobile application of the recipient.

(4) When using API integration, successful sending shall be considered the receipt of the electronic message on the Evrotrust backend (server) through the built API interface, and successful delivery shall be considered the receipt of the sent electronic content in the information system of the recipient through such interface.

(5) When using a web-based portal, successful sending shall be considered the receipt of the electronic message from the web browser of the Subscriber using the portal on the Evrotrust backend (server), and successful delivery shall be considered the receipt of the sent message in the virtual mailbox accessible in the recipient's account through the web-based portal.

(6) When using the qualified REM service, successful sending shall be considered the time of receipt of the electronic message in the information system on the Evrotrust electronic mail server (backend), and receipt shall be considered the receipt in the electronic mailbox serviced by the Evrotrust electronic mail server.

2.7.3.2. Evrotrust makes sure that the service protects the electronic content being transmitted against loss, theft, breach of integrity or unauthorized alteration and meets the requirements of Regulation (EU) № 910/2014.

2.7.3.3. The period of time during which the sent electronic content is available and the electronic registered mail system is making attempts to deliver it shall be set in advance by the sender. Should the sender fail to select an option, then such period shall by default be equal to 3 (three) days.

2.8. QUALIFIED PRESERVATION OF QUALIFIED ELECTRONIC SIGNATURES/SEALS AND/OR ELECTRONICALLY SIGNED/SEALED ELECTRONIC DOCUMENTS

The Qualified Preservation Service for Qualified Electronic Signatures (PSES) and the Qualified Preservation Service for Qualified Electronic Seals (QPSES), OID:

1.3.6.1.4.1.47272.2.13, are provided by Evrotrust in accordance with Art. 34 and Art. 40 of Regulation (EU) № 910/2014.

These trust services provide for secure and reliable long-term preservation of any type of electronic signatures and seals affixed to documents (without storing the documents themselves in a depository) and/or electronically signed/sealed documents (with a depository) of Subscribers of the service, and provides evidence of the preservation process, with the possibility to validate the electronic signatures/seals in the long run. In the provision of those services, Evrotrust shall fulfil requirements related to the procedures and technologies used that are capable of extending the reliability of the qualified electronic signature/seal beyond the period of its technological validity. These requirements are set out in applicable standards, for which Evrotrust has been certified by an independent conformity assessment body.

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. They can be provided separately or in an I/O (input/output) package that is reliably protected by encryption. In any case, they shall only be transmitted to either the Subscriber or its authorized representative. Evrotrust maintains information on all prepared I/O packages, including the date of the event and the criterion under which the stored objects included in the package have been selected. The request must indicate the person requesting the data, the reasons for requesting it and the method in which it wishes to receive it, for example, by e-mail or on an electronic medium. Evrotrust reserves the right to approve or refuse the execution of the request, without being required to motivate its refusal, or to notify the requester thereof, except in the cases specified in a legislative act. For the purpose of providing the data and evidence, Evrotrust may collect fees to ensure the execution of the submitted request. Evrotrust does not use any external organizations supporting the preservation service. At the end of the data preservation period, the data will be deleted.

2.8.1. Specific requirements to the provision of a qualified preservation service for qualified electronic signatures/seals

(1) The qualified preservation service keeps a preservation schemas and profiles which are related to the evidence generation and validation policies, as well as the extension of the period of validity and the validation of signatures. The preservation schemas and profiles has

identifiers that uniquely identifies them.

(2) Evrotrust QPSES maintains the following preservation profiles:

a. Qualified preservation service profile for any documents/data (F2.1) under a preservation scheme with temporary storage based on an archival time assertion (F2).

b. Qualified preservation service profile on SHA-512 for any documents/data (F2.2) under a preservation scheme with temporary storage based on an archival time assertion (F2).

c. Qualified preservation service profile for electronically signed documents (F3.1) under a preservation scheme with extension of the reliability of electronic signatures/seals and with storage(F3).

(3) With regard to the use of the stated trust services, Subscribers shall, among the other obligations provided for in these General Terms and Conditions, have the following specific obligations and responsibilities:

a. to get acquainted with and observe the terms and conditions of the applicable Policies and Practices, as well as the requirements set out in the other documents published in the Evrotrust's website;

b. to use the qualified preservation service only for lawful purposes and in accordance with the Policy and Practice determined therefor;

c. to approve the terms and conditions set out in these General Terms and Conditions, which constitute the contract between them and Evrotrust. These General Terms and Conditions indicate who has the right to access the stored objects, including the sent data objects and evidence, and who has the right to monitor the actions related to the stored objects.

(4) Clients may submit a request for I/O packages by using an e-mail, an mobile application of Evrotrust, a web application or through physically visiting an office of a Registration Authority of Evrotrust.

(5) In case Evrotrust is unable to collect and verify all data for the validation of the accepted document and the evidence, it will send an indication of a failed operation.

(6) When the person, that is using the service, provides hash values which might be used in a hash-tree-renewal, Evrotrust is not liable for guaranteeing that the new hash values correspond to the original hash values of the hash tree. Evrotrust has no way of knowing to which document the hash values correspond and even if it really corresponds to a hash value of a

concrete hash computation.

(7) When the person, that is using the service, provides hash values of objects to preserve, and not the object itself, the preservation is only on the submitted objects and that this allows a proof of the existence of the hashed object only as long as the hash algorithm is strong enough.

(8) The person that is using the service is not allowed to take a role in the preservation process (e.g. providing needed validation data).

(9) The supported preservation service policies are described in detail the the applicable Policies and Practices.

2.9. ELECTRONIC IDENTIFICATION

A Subscriber of the electronic identification service is the individual who identifies itself, regardless of whether the fee for the provision of the service is paid by itself or by the Relying Party. When providing the electronic identification service, Evrotrust, on assignment by the Subscriber, creates a document with its identification data in such volume as is necessary for its identification before a given Relying Party. The generated volume of identification data may include a copy of the Subscriber's identity document and other graphic elements (photograph, specimen, etc.) electronically certified as being "true copy of the original", if the production of such a copy is required by the Relying Party for the purposes of the Subscriber's identification (e. g. an individual Relying Party obliged to apply anti money laundering measures). The provision of the electronic identification service also includes the generation of a pair of cryptographic keys for a qualified electronic signature and the issuance of a short-term attributive QESQC under item 2.1.2, whereby the Subscriber signs the generated electronic identification document. The short-term attributive QESQC issued under item 2.1.2 whereby the Subscriber signs the generated electronic document contains all personal data which Evrotrust has made sure to be up-to-date and has verified using legally permissible means under Regulation (EU) № 910/2014. By the short-term attributive QESQC issued, the document for self-declaration of circumstances by the Subscriber is signed remotely. It serves only for the purposes of identification, insofar as the attributive QESQC binds Evrotrust with responsibility for the validity of the circumstances entered therein. When the provision of the electronic identification service has been requested in an office of a Registration Authority of Evrotrust, the attributable QESQC issued may also be used for

signing the contract for the provision of such service, together with these General Terms and Conditions and the applicable Evrotrust Personal Data Protection Policy.

2.10. ELECTRONIC AUTHENTICATION

A Subscriber of the electronic authentication service is the individual identifying itself before the Relying Party, regardless of whether the fee for the provision of the service is paid by itself or by the Relying Party. When providing the electronic authentication service, Evrotrust, on assignment by the Subscriber, generates a document with structured content containing identification data of the Subscriber in such volume as is necessary for its identification before a given Relying Party for the needs of its access to specific content provided by the latter, and the so generated document is then sent to the Relying Party without being signed.

3. LIMITATIONS ON THE USE OF THE SERVICES PROVIDED

The Subscriber undertakes to take all necessary actions in order to minimize and limit the damages resulting from the use of the services exceeding the limitations on their use as specified in these General Terms and Conditions. Relying Parties agree and undertake to take all necessary actions, when relying on an electronic identification service or a trust service provided by Evrotrust, to keep track of and observe the limitations on the use of the services as set out in these General Terms and Conditions.

3.1 TIME LIMITS

Each certificate issued by Evrotrust may only be used until the expiry of its validity. The period of validity of the certificates is entered therein.

Where a certificate has been cancelled, the Signatory /Creator shall not use the private key to create an electronic signature/seal.

3.2 INTENDED PURPOSE

Certificates issued by Evrotrust shall be used in accordance with their intended purpose as described in these General Terms and Conditions, in the applicable Evrotrust Policies and Practices and in the applicable law.

The verification of the intended purpose of a certificate shall be performed based on the

following data contained in the certificate profile:

(1) Policy/Practice in accordance with which an electronic signature/seal certificate is issued and managed, as specified in the "Certificate Policies" field;

(2) the intended purpose and limits on the effect of the certificate with respect to the purposes for which it is used, as described in the "Key Usage" and "Extended Key Usage" fields;

(3) details of the Certificate Signatory /Creator, as specified in the "Subject" field.

3.2.1 TRANSACTION VALUE

The issued qualified certificates for qualified electronic signature/seal are normally intended to be used for transactions worth up to EUR 20,000 (twenty thousand euros), unless a certificate stating a higher value of the transactions has been issued. The issued qualified certificates for advanced electronic signature are intended to be used for transactions worth up to EUR 500 (five hundred euros). The applicable limits on the value of the transactions for which the issued qualified electronic signature/seal certificate is intended to be used shall be recorded in the „id-etsi-qcs-QcLimitValue" attribute/field in accordance with the requirements of ETSI EN 319 412-5 and may are verified by each Relying Party. Signed documents for transactions with values higher than the established limit will de-qualify the signature as being "qualified" and it can be converted into either advanced or ordinary with the ensuing legal consequences. In such cases, the risk and responsibility shall be entirely borne by the Signatory /Creator. Evrotrust shall not be liable for any damages resulting from the use of qualified electronic signature/seal certificates issued by it for transactions exceeding the stated transaction value limits. The risk associated with the acceptance of electronic documents signed with qualified electronic signatures/accompanied by electronic seal certificates, with a material value exceeding the transaction value limits stated in the certificate, shall be entirely borne by the Relying Party.

4 SPECIFIC CONDITIONS FOR QUALIFIED TRUST SERVICES ISSUANCE

4.1 ACCEPTANCE OF A CERTIFICATE

4.1.1. Upon receipt of a qualified certificate, the Subscriber shall be obliged to verify its content with regard to the accuracy of the data and the existence of a public key corresponding to the private key it holds.

4.1.2. If any incorrect data has been entered in the certificate, the certificate shall be immediately cancelled. If the Subscriber objects that the qualified certificate issued contains errors or omissions within 3 (three) days from its publication in the certificate repository, Evrotrust will remove it by issuing a new certificate at no cost, unless they come as the result of the provision of incorrect data. If no objection has been made, the content of the certificate shall be deemed to have been accepted. The rules contained in this item shall apply both to the issuance of a certificate and to the renewal of a certificate. In case of remote issuance of a certificate through a mobile application of Evrotrust, if the Subscriber finds any inaccuracies in the data entered, it may at any time activate the functionality for cancellation of the certificate and for immediate issuance of a new certificate free of charge.

4.1.3. A qualified certificate shall be considered to have been accepted by the Subscriber where any of the following prerequisites exists:

(1) Explicit approval/confirmation by the Subscriber;

(2) The qualified certificate has been used for the first time by the Subscriber; or

(3) After the expiry of 3 (three) days from the date of issuance of the qualified certificate, if within the said period the Subscriber has not made an objection regarding the content of the certificate.

4.1.4. In the case of certificates of electronic signature, or electronic seal respectively, the obligation under item 4.1.1, the possibility of objection under item 4.1.2, and the prerequisites under which the certificate is considered to have been accepted under item 4.1.3, shall at all times apply only in respect of the Signatory, or the Creator respectively, regardless of whether the issuance of the certificate itself is paid by them or by a third party (another Subscriber) which has also entered into a contractual relationship with Evrotrust under these General Terms and Conditions.

4.1.1 PERIOD OF STORAGE OF CONTRACTS AND ANY OTHER INFORMATION RELATED TO THE IDENTIFICATION OF THE SIGNATORY/CREATOR/SUBSCRIBER

All information relevant to and all data created or received by Evrotrust in relation to the

process of Subscriber identification and registration and/or the conclusion of a contract under these General Terms and Conditions for the provision of trust services (incl. evidence of the conclusion thereof and of the acceptance of the General Terms and Conditions) will be recorded and stored by Evrotrust for the entire period of validity of the respective contract and for a period of 10 (ten) years after the termination thereof. Within the said period, information on each certificate issued, cancelled and revoked by Evrotrust will be stored as well, and the period shall commence from the revocation of the certificate. The same period shall also apply to information created or received by Evrotrust in relation to the process of provision of validation services, qualified e-mail, qualified signature/seal storage, electronic identification and electronic authentication, including logs for all events associated with the issuance, effect and validity of the keys, incl. information on each generated key pair. Such information will be stored for the period specified herein, including after Evrotrust has ceased its activities. Such information is stored in order for Evrotrust to fulfil its legal obligations under Art. 24 (2) (h) of Regulation (EU) № 910/2014 and the standards applicable to its activities, and with the purpose of providing evidence in legal proceedings and ensuring continuity in the provision of the service.

5 SUBSCRIBER, SIGNATORY, CREATOR AND RELYING PARTIES

5.1 SUBSCRIBERS

5.1.1. A Subscriber is an individual or legal entity that is bound by a contract with Evrotrust, whereunder Evrotrust provides it with trust services. A Subscriber may also be a person other than a Signatory of electronic signature/Creator of seal, however the conclusion of a contract with Evrotrust under these General Terms and Conditions is a mandatory condition for each Signatory of electronic signature/Creator of seal for the issuance of a certificate by Evrotrust. The Subscriber may act on behalf of one or more different Signatories/Creators with whom it is affiliated (e.g. a legal entity that pays for the issuance of electronic signature certificates for its employees). The Subscriber may not be stated in the data entered in the issued certificate. The Subscriber may also be a person who, for example, uses a trust service of Evrotrust such as time-stamp.

In cases where the Subscriber is a person other than the Signatory (e.g. one person requests services in favor of other persons), the Subscriber shall accept these General Terms and Conditions, but at the same time, it shall also enter into a contract containing additional individual

arrangements with Evrotrust. In such cases:

1. identification of the Signatory shall be made in a way that does not differ from the way in which such persons are identified when they are the sole Subscribers and directly enter into contractual relationships with Evrotrust;

2. both the Subscriber and the Signatory/Creator shall enter into a contract with Evrotrust under these General Terms and Conditions.

5.1.2. A Signatory of an Electronic Signature/Signatory is the individual creating the electronic signature. Details about the Signatory shall be entered in the electronic signature certificate.

5.1.3. A Creator of a seal/Creator is a legal entity creating an electronic seal. Details about the Creator of a seal shall be entered in the electronic seal certificate.

5.1.4. The Signatory/Creator is the person indicated in the certificate as the Signatory of the private key associated with the public key (Subject within the meaning of ETSI EN 319 411-1).

5.1.5. A Relying Party means an individual or legal entity who relies on electronic identification or a trust service provided by Evrotrust.

5.2 SIGNATORY OF ELECTRONIC SIGNATURE

Through an issued electronic signature certificate, a Signatory may make on its own behalf or on behalf of another person it represents, electronic statements which it signs electronically, in accordance with the representative power vested in it. The electronic signature certificate may also indicate the person represented by the Signatory. Only the Signatory stated in the certificate shall have the right to access the private key through which it creates an advanced or qualified electronic signature.

5.3 CREATOR OF AN ELECTRONIC SEAL

A Creator may sign electronic objects, regardless of their nature (software, photographs, music, films, books, architectural projects, databases, design, etc.), thereby declaring that it is the

legitimate source of such electronic object, as well as that the object has intact integrity. An electronic seal does not guarantee the Creator any rights over the electronic object (copyright and others). A legal entity Creator of an electronic seal shall be entered in the issued electronic seal certificate as the Creator. Only empowered persons designated by the Creator entered in the certificate shall have the right to access the private key for signing electronic statements through which an advanced or qualified electronic seal is created.

5.4 RELYING PARTIES

5.4.1. Relying Parties shall have knowledge and skills regarding the use of a qualified certificate and rely on the certified circumstances therein only in view of the applicable Policies and Practices, especially with regard to the level of certainty when verifying the identity of the Signatorys and the identity of the Creators of such qualified certificates, as well as with regard to the limitations on its use as stated in the certificate.

5.4.2. The Relying Parties shall have permanent access to the Evrotrust registers to verify the validity of qualified certificates or other circumstances and data reflected in the certificates or entered in those registers.

5.4.3. Due care by Relying Parties

Each Relying Party shall take due care, by:

(1) relying on a certificate only in view of its intended purpose and the limitations under which it was issued, in accordance with the applicable Evrotrust Policies and Practices, the information entered in the certificate itself and the provisions of these General Terms and Conditions;

(2) verifying the status of the certificate by using online certificate status protocol (OCSP) service maintained by Evrotrust. A verification of the electronic authenticity and integrity of the certificate outside the OCSP service or in an outdated Certificate Revocation List (CRL) does not provide verification of its validity and all damages caused by actions taken after such verification only shall be borne by the Relying Party;

(3) verifying the validity of the electronic signature/seal of electronically signed statements, as well as the validity of the electronic signature of Evrotrust along the certificate chain

up to the base certificate;

(4) making sure that the applications using the certificate are functionally applicable for the purpose for which it was issued, and in view of the level of security, as set out in the relevant Policies and Practices;

(5) verifying that the signature/seal accompanied by the certificate has not been used for the purposes and for the value of transactions beyond the limits and purposes stated in the certificate;

(6) making sure that the length of the keys used meets the security requirements of the Relying Party;

(7) making sure that the certificate was valid at the time of creation of the electronic signature/seal.

The Relying Party's due care is expressed in its using a mechanism for secure verification of an electronic signature/seal, which ensures that:

(1) the public key used to verify the signature/seal corresponds to the one produced before it;

(2) the verification for the use of the private key has been reliably confirmed and the results of such verification are correctly presented;

(3) where necessary, the content of the signed electronic document may be established;

(4) the authenticity and validity of the certificate at the time of signing are reliably confirmed;

(5) the results of the verification and the electronic identity of the Signatory/Creator are correctly presented;

(6) any security-relevant changes are detectable.

Evrotrust shall not be liable for any damages incurred by the Relying Party due to failure to take due care.

5.4.4. Verification of certificates

The verification of electronic signature and electronic seal certificates issued by Evrotrust is performed using the status verification services and the Certificate Revocation Lists kept by

Evrotrust. The verification of time stamps certificates is performed by verifying their compliance with the standard under which they were issued. All electronically signed documents, including validation reports, can be verified using the validation service provided by Evrotrust (https://www.evrotrust.com/landing/bg/a/validation). The Evrotrust system used for validation of qualified electronic signatures/seals provides the Relying Parties with the correct result of the validation process and allows them to detect any security-related issues.

Each Relying Party, upon receipt of an electronic document signed with a qualified electronic signature/seal by a Signatory/Creator, shall verify the status of the qualified certificate in the current Certificate Revocation List (CRL) or by a verification of the current status of the certificate in real time (OCSP) or through a qualified electronic signature/seal validation service provided by Evrotrust. For the avoidance of doubt, the certificates issued by Evrotrust contain a period of validity which a Relying Party must always comply with before relying thereon. A Relying Party shall only rely on a certificate until it is cancelled. A Relying Party shall not rely on a certificate where the signature/seal was created at a time the certificate had been cancelled. Each document bearing a defective or suspicious electronic signature/seal shall be rejected or possibly subjected to further procedures that allow for its validity to be indicated. The Relying Party shall also take all other precautionary measures as provided for in these General Terms and Conditions or in any other applicable Evrotrust document. Any person who approves such a document shall be responsible for any consequences resulting thereafter.

An update of the current Certificate Revocation List (CRL) shall be automatically done not later than every 3 (three) hours or immediately after the cancellation or revocation/renewal of a valid certificate. In all Certificate Revocation Lists (CRLs) Evrotrust indicates the time for the next issue. The effective period of validity of the current published List is indicated therein. Evrotrust keeps in its Certificate Revocation Lists information about all the revoked certificates issued by the respective certification authority regardless of their validity period. Evrotrust CRLs include the X.509 „ExpiredCertsOnCRL“ extension as defined in ISO/IEC 9594-8/Recommendation ITU-T X.509. Evrotrust shall not issue a last CRL until all certificates in the scope of the CRL are either expired or revoked.

Any Relying Party, upon accepting a qualified certificate, may request a real-time certificate status verification using the OCSP (On-line Certificate Status Protocol) service. Such verification, unless a real-time update of the qualifying certificate status is done, is not mandatory

for the Relying Parties. However Evrotrust recommends using this OCSP service. To achieve higher security when using electronic signatures/seals, it is recommended to integrate the service in the process of creating or accepting electronically signed documents. The OCSP service must be provided by Evrotrust.

5.4.5. In case of breach of the security of the private key (its disclosure) of the Certification Authority or other entities operating within Evrotrust, Evrotrust shall immediately inform the Relying Parties by publishing information on its website.

5.4.6. The Evrotrust public keys are published in the certificates of the Evrotrust Certification Authority in X.509 v.3 format. The certificates are published in the certificate repository and accessible via the Evrotrust's website at: https://www.evrotrust.com. Each Relying Party builds trust in Evrotrust by accepting and installing in the systems under its control the operational certificates of Evrotrust.

5.4.7. Evrotrust maintains certificate repository (where it publishes the certificates it uses in its activity as a trust service provider, the issued certificates and the certificate revocation list.

5.4.8. Evrotrust shall not be liable for any damages caused by the failure of a Relying Party to comply with the requirements set out in these General Terms and Conditions. Evrotrust's relations with the Relying Parties shall be governed by the common tort law in accordance with the applicable law.

6 CONTRACT. CONCLUSION. SUBJECT MATTER OF THE CONTRACT

Evrotrust shall provide, either free of charge or for a fee, the services covered by these General Terms and Conditions, subject to and in strict compliance by the Subscriber/Signatory/Creator of the contract entered into under these General Terms and Conditions, as well as the applicable law. The services are diverse, constantly supplemented and modified with a view to their improvement and expansion and on this basis, their number, characteristics and the conditions for their provision may be unilaterally changed at any time by Evrotrust within the limits provided by the applicable law.

6.1 WAYS FOR REQUESTING A SERVICE AND ENTERING INTO A CONTRACT. REGISTRATION

The services of Evrotrust may be requested and, respectively, provided in different ways depending on their nature and in accordance with these General Terms and Conditions. The requesting of a service and the conclusion of a contract requires the Subscriber's secure identification in accordance with the level of security required for the specific service and the Subscriber's acceptance of these General Terms and Conditions. Before requesting a service, the Subscriber shall get acquainted with all the Policies and Practices applicable to the relevant service. Upon requesting a service, the Subscriber accepts these General Terms and Conditions.

The different services of Evrotrust may be requested in different ways and not every way of requesting provides an opportunity to request each of the services. Evrotrust maintains up-to-date information on the ways to request and use the different types of services on its website.

Evrotrust services may be requested in any of the following ways:

6.1.1. In person at an Evrotrust office:

The procedure for requesting a trust service in an Evrotrust office requires the Subscriber's physical presence, in cases where the Subscriber is an individual, or respectively the presence of a legal representative or a proxy duly authorized by a notarized power of attorney, in cases where the Subscriber is a legal entity.

6.1.1.1. Individual Subscriber

The Subscriber shall provide the following information for unambiguous identification and verification of its identity: Full name (as in the identity document); identity document – personal ID card, international passport or other identity document; National Identification Number, if any; contact details - mobile phone number, e-mail address and postal address. A copy of the identity document will not be taken. After successful verification of the Subscriber's identity, an authorized operator from the Evrotrust internal Registration Authority will:

(1) propose a contract for qualified trust services signed on behalf of Evrotrust, and keep all submitted documents relating to the contract. The contract will be signed by the

Subscriber on paper together with these General Terms and Conditions, with the applicable Evrotrust Personal Data Protection Policy and all other documents relevant to the requested service.

(2) confirm the request for issuance and send an electronic request for the issuance of a certificate to the Evrotrust operational Certification Authority;

(3) record the issued certificate on a Secure Signature Creation Device (QSCD) and transmit it to the Signatory or to the authorized person (if applicable).

6.1.1.2. Legal Entity Subscriber

The establishment of the identity of a legal entity is performed by the Registration Authority, through a verification in the relevant registers based on a provided registration or other unique identification number of the legal entity. The identification of legal entities and the verification of the representative power is performed on site on the basis of information provided by the Subscriber through automated remote identification. In such identification, all data that will be entered in the issued certificate, as well as the legal representative power of the person who appeared in the office of Evrotrust, are verified in real time.

For legal entities for which an automated verification cannot be performed, the following shall be submitted:

(1) Court decision or other document certifying the establishment of the legal entity;

(2) Document certifying the entity's good standing;

(3) Unique national identifier;

(4) Other relevant documents.

After copying all the required documents, with the consent of the person who submitted the request, the copies remain in the Evrotrust records. For the avoidance of doubt, such consent shall not constitute consent under Regulation (EU) № 679/2016, but rather a contractual consent and shall be a mandatory condition for the conclusion of the contract. The certification of the information contained in the documents submitted shall be performed by „True copy of the original" certification and handwritten signature affixed on the documents before an officer of the Registration Authority by the person representing the Subscriber, in case of personal delivery of the documents. The certification of the identity of a legal entity has two purposes: (1) verification of whether or not the legal entity exists at the time of reviewing the request and (2) verification of

whether or not the person appearing on behalf of the legal entity has the necessary representative power to request the relevant trust services and to validly enter into the contract for the provision thereof under these General Terms and Conditions on behalf of the Subscriber.

When identifying persons for whom certificates are issued for the purposes of fulfilling the requirements of PSD2, Evrotrust will verify the specific attributes which it receives from the person and which it enters in the certificates issued, by using authentic information from a National Competent Authority (NCA) (e.g. a public register). In the event that the NCA has established rules for the verification of such attributes, Evrotrust shall implement and apply them.

Evrotrust makes sure that individuals and legal entities are correctly identified, their identity is verified and that the requests for the issuance of qualified certificates are duly verified and approved, including the full name and legal status of the individual/legal entity concerned and the link between the certified data and the individual/legal entity.

6.1.2. In person at an office of an external Evrotrust Registration Authority:

The procedure for requesting a service and entering into a contract commences with the personal appearance of the individual Subscriber or a legal representative or a duly authorized proxy of the legal entity Subscriber at an office of an external Registration Authority and the filing by the Subscriber of a request with the Registration Authority for the respective service. A request may be filed with an external Evrotrust Registration Authority for any of the Evrotrust services in respect of which the relevant external Registration Authority is authorized to act as an Evrotrust Registration Authority. Upon the appearance of the Subscriber before the Registration Authority, the following procedure for requesting a service will be performed:

6.1.2.1. in the manner described herein above in item 6.1.1, where the service is requested and accordingly the contract is entered into on hard copy;

6.1.2.2. a short-term QESQC issuance service shall be requested in the sequence indicated herein below:

(1) The Registration Authority will acquaint the Subscriber with the General Terms and Conditions under which the contract is to be concluded, together with the content of the request for the issuance of a certificate, the applicable Evrotrust Policies and Practices and the applicable

Evrotrust Personal Data Protection Policy.

(2) The Subscriber will produce before the Registration Authority an identity document in order to be identified and to have a short-term QESQC issued;

(3) The Registration Authority will perform identification of the Subscriber by comparing the photograph from the produced identity document with the physically present person who appeared before the Registration Authority;

(4) In case there is a match between the photograph on the identity document and the physically present person, the Registration Authority will record, from the identity document produced by the Subscriber and enter in the Evrotrust information system, identification data related to the Subscriber: full name, unique identification number (if any) and/or the number of the identity document;

(5) Based on the data entered in the Evrotrust information system by the Registration Authority, Evrotrust will perform additional identification of the Subscriber through verification, in the databases of the official primary data controllers in the respective country (e.g. the databases of the authority that issued the identity document), of the correctness of the entered data and the validity of the identity document produced before the Registration Authority;

(6) In addition to the entered data, the Subscriber will provide, for the purposes of concluding the contract, details of its valid mobile phone number and e-mail address which must be under its sole control. For the avoidance of doubt, a PIN code and a secret link for activation of and signing with the short-term QESQC issued by Evrotrust will be sent to the mobile phone number designated by the Subscriber, and the contract signed by the Subscriber, as well as the applicable Evrotrust Personal Data Protection Policy, will be sent to the e-mail address designated by the Subscriber.

(7) The Registration Authority will send to Evrotrust a request signed by it for the issuance of a short-term QESQC and will confirm the performed identification of the Subscriber.

(8) Upon successful identification of the Subscriber confirmed and signed by the Registration Authority, Evrotrust will issue the requested short-term QESQC in real time and will send via SMS to the mobile phone number designated by the Subscriber a PIN code and a secret link for activation of and signing with the issued QESQC. For security reasons, the sent code and the secret link for activation and signing will be valid and can be used for activation and signing purposes for a limited period of time only, and when the said period expires, they can no longer

be used and the requested short-term QESQC will not be issued. A short-term QESQC issued under the above procedure can be used to sign the request for the issuance of a certificate, the General Terms and Conditions and the applicable Evrotrust Personal Data Protection Policy. Upon signing those documents, the signed request together with the General Terms and Conditions will form the contract between Evrotrust and the Subscriber.

(9) The Subscriber will sign the contract by entering the PIN code in the space/field indicated by the Registration Authority, marking the appropriate field for acceptance of the General Terms and Conditions and for confirming that it is familiar with the Evrotrust Personal Data Protection Policy, and will press the „Sign" button through the Registration Authority's device in the Evrotrust information system; or, alternatively, by clicking on the secret active link received in an SMS message sent to it. By performing one of the actions referred to above, the Subscriber declares that it is familiar with the applicable Evrotrust Personal Data Protection Policy pursuant to which Evrotrust processes its personal data in relation to this contract, declares that it is familiar with and accepts these General Terms and Conditions and thus is entering into a contract with Evrotrust under these General Terms and Conditions for the requested service. At the same time, the Subscriber will also sign with the short-term QESQC the documents of the Relying Party that have been submitted for signature by the Relying Party. Upon the entering of a PIN code or, respectively, clicking on the secret link and receiving a signed request from the Registration Agent, the short-term QESQC will be activated and, through the Evrotrust information system, a request will be made by the Subscriber for the signing of the documents described above. Upon the said signing, the contract will be considered to have been entered into, and the requested services will be considered to have been fully provided. In case of refusal by the Subscriber to sign the contract with Evrotrust or, respectively, in case of refusal by or inability of (regardless of the reason why) the Subscriber to enter a PIN code or to click on the secret link, the short-term QESQC will not be issued. Evrotrust will immediately confirm the signing of the documents to the Subscriber, and the Relying Party will be obliged to serve them on the Subscriber.

(10) Evrotrust will immediately deliver (send) on behalf of the Subscriber the electronic documents signed by the Subscriber with the short-term QESQC, intended for the Relying Party, to the latter.

6.1.3. Remotely via mobile application of Evrotrust.

The terms and procedure for requesting a trust service and concluding a contract via an Evrotrust mobile application are regulated in Section 7 of these General Terms and Conditions.

7 EVROTRUST'S MOBILE APPLICATIONS

7.1 INSTALLATION OF THE EVROTRUST MOBILE APPLICATION

In order to use the services via the Evrotrust mobile application, the Subscriber shall agree in advance with these General Terms and Conditions and the Contract for Use of Service Accessible through the Application of Evrotrust and perform the steps described below:

(1) to have a device that enables the installation and normal operation of the respective version of the Evrotrust mobile application. The mobile application may require that the access to the device used for its installation be secure and have functionality for access to the device through biometrics (e.g. fingerprint, facial recognition, and the like);

(2) to have ensured that the device used by it is connected to the Internet in a manner that enables it to use data transmission services at a speed that allows functional access to the Internet;

(3) to have ensured a device's connectivity to a mobile network in a manner that enables it to use mobile services, including the possibility to receive and send short text messages (SMS), IM messages, and e-mail;

(4) to have the latest updated version of the Evrotrust mobile application installed on the device and to keep the installation up to date.

7.2 CONTRACT CONCLUSION ACTIONS

7.2.1. After the mobile application has been installed and started on the device, the Subscriber will get acquainted with and accept the General Terms and Conditions and the Contract for Use of Service Accessible through the Application of Evrotrust, confirm that it has read the applicable Evrotrust Privacy Policy, give its explicit consent to the processing of its biometric data and to decision making based on automated processing of personal data in accordance with the Declaration of Consent for automated processing of biometric personal data, and activate the mobile application by pressing the appropriate button clearly indicating the acceptance of the terms of the contract or proceeding with the installation. By doing this, the

Subscriber makes a request to Evrotrust to take action for the conclusion of a contract under the terms of the Contract for Use of Service Accessible through the Application of Evrotrust, an integral part of which is a request for remote issuance of a QESQC. These General Terms and Conditions are integral part of the Contract for Use of Service Accessible through the Application of Evrotrust.

7.2.2. By the actions under item 7.2.1, the Subscriber agrees that the communication with it will be executed through the e-mail address and mobile phone number indicated by it during its registration, including through IM messages through the mobile application and short text messages (SMS). Each successfully sent message to the indicated e-mail, mobile phone number will be considered duly served, without being necessary to confirm the receipt thereof. The successful sending of a message to the Subscriber through the mobile application will be considered secure and proper delivery of electronic registered mail within the meaning of Regulation (EU) № 910/2014.

7.3 REGISTRATION IN EVROTRUST MOBILE APPLICATION

The Subscriber's registration in the Evrotrust mobile application includes the following steps:

7.3.1. Security codes

When starting the application, the Subscriber selects and enters its PIN code and secret word. The secret word is used to restore a forgotten PIN, to change the PIN or to change the information about the Subscriber's registration.

The PIN code is secret and in no way reaches Evrotrust, nor is it stored in the mobile application. The Subscriber is not allowed to disclose its PIN code to third parties. If the Subscriber does so, then all statements will be considered to have been made by it, with the ensuing legal consequences binding on its legal field.

Within the Evrotrust mobile application and only in it, depending on the supported functionality of the device on which the application is installed, as well as the software functionalities developed by Evrotrust, biometric data of the Subscriber can be linked to the PIN code - fingerprint, face shape, etc. The Subscriber's biometric data remains under its control at

all times within its device and the installed application. It is not processed and stored by Evrotrust. The Subscriber may at any time stop using these functionalities.

7.3.2. Entering personal data

The Subscriber shall enter its personal data as follows:

a) After creating the security codes, the Subscriber shall enter its personal data according to the fields provided in the Evrotrust application and confirm its accuracy by clicking the "Next" button. By this action, the data is automatically sent to the Evrotrust system;

b) The Subscriber will have the opportunity to correct the entered data by clicking the „Next" button.

7.3.3. Identification

The Subscriber's identification and the verification of the data provided by it shall be performed as follows:

a) The Subscriber shall capture a clear copy of its valid identity document using the camera of its device and send it to the Evrotrust system via the mobile application, following the shooting instructions.

b) The data from the identity document will be automatically recognized by the Evrotrust system.

7.3.3.1. Automated identification:

(1) Where it is technologically feasible, Evrotrust will perform an automated verification of the Subscriber's identity through a respective exchange of the data established under item 7.3.3 (b) above with the registers of the primary data controllers in the respective country who issued the identity document, in case such access is provided by the jurisdiction of the identity document issuing country.

(2) When using an identity document with an NFC chip, the identification will rely on data retrieved by means of an NFC chip on the Subscriber's identity document.

(3) The Subscriber shall capture its face using the camera of its device according to the instructions which will be visualized on the screen of the mobile application.

(4) Where it is technologically feasible, automated identification will be performed, the taken biometrics of the Subscriber's face being automatically compared with the Subscriber's photograph obtained under the terms of item 7.3.3.1., para. (1) or para. (2);

(5) Upon successful verification of the validity of the identity document and successful identification under item 7.3.3.1, para. (4), it is considered that the Subscriber has been successfully identified and its identity has been verified.

7.3.3.2. Semi-automated identification.

Upon unsuccessful automated identification, as well as in case of lack of integration with the registers of the primary data controllers in the respective country who issued of the identity document, a real-time videoconference call will be held through the mobile application between the Subscriber and an Evrotrust operator. Upon successful identification by the operator, the latter will confirm the Subscriber's identification and identity. If there are publicly available registers for verification of the validity of the identity document or the status of the person, such verification will be performed ex officio.

7.3.4. Contact details

Upon successful identification, the Subscriber shall fill in contact details as per the electronic form in the mobile application.

7.3.5. Confirmation of the registration and conclusion of the Contract

The conclusion of a contract between the Subscriber and Evrotrust requires confirmation of the registration by the Subscriber:

a) To complete the registration process, the mobile application will send to the mobile phone number and e-mail address designated by the Subscriber messages with 6-digit confirmation codes;

b) Upon the successful entry and acceptance of the codes by the Evrotrust system, the Subscriber shall press the "Confirm" button whereby it requests from Evrotrust the issuance of a QESQC and makes a request for signing the contract.

c) By performing the actions under (b), the Subscriber requests from Evrotrust the remote QESQC issuance service, and Evrotrust will issue the Subscriber a QESQC in real time and

ensure the signing with a qualified electronic signature of the General Terms and Conditions, the Contract for Use of Service Accessible through the Application of Evrotrust, the applicable Personal Data Protection Policy and the Declaration of Consent. For the avoidance of doubt, by pressing the "Confirm" button under (b), the Subscriber enters into a contract under the terms of the Contract for Use of Service Accessible through the Application of Evrotrust and these General Terms and Conditions and it is considered to have been entered into, and the registration process will be completed;

d) The contract signed by both the Subscriber and Evrotrust will be sent to the Subscriber through the mobile application;

e) The wording of the contract (the General Terms and Conditions and the Contract for Use of Service Accessible through the Application of Evrotrust) shall be available for storage on the Subscriber's device in a way that allows its download and storage on a local device, as well as subsequent reproduction in the "Settings" menu of the application and on the Evrotrust's website. The contract will be concluded in Bulgarian or in another language supported by the mobile application and selected by the Subscriber. By selecting the language of registration by the Subscriber, it is assumed that the Subscriber understands such selected language.

7.4 REGISTRATION IN THE MOBILE APPLICATION „ID, OPERATED BY EVROTRUST" (ID)

The Subscriber's registration in the Evrotrust mobile application „ID, operated by Evrotrust" includes the following steps:

7.4.1. Choice of language

By selecting the language of registration, it is assumed that the Subscriber understands such selected language.

7.4.2. Contact details

The Subscriber shall enter its mobile phone number and valid e-mail address. The application will send a message with a 6-digit confirmation code to the mobile phone number designated by the Subscriber. Upon the successful entry and acceptance of the code by the Evrotrust system, the Subscriber shall press the „Confirm" button.

7.4.3. Identification:

7.4.3.1. Identity document

The Subscriber shall capture a clear copy of its valid identity document using the camera of its device and send it to the Evrotrust system via the mobile application, following the shooting instructions. The data from the identity document will be automatically recognized by the Evrotrust system. The Subscriber shall verify the correctness of the data automatically read by and uploaded on the Evrotrust system and confirm it by pressing the "Confirm" button in case it fully corresponds to its data as per its identity document.

In the event that there is no integration with primary national registries for verification of the validity of the identity document and an identity document with an NFC chip is used, the data will be retrieved by reading the chip. For this purpose, the Subscriber shall press its document against the device. After retrieving the data from the NFC chip, its subsequent editing by the Subscriber is not allowed.

7.4.2.2. Automated identification:

(1) The Subscriber shall capture its face using the camera of its device according to the instructions visualized on a screen in the mobile application. The taken biometrics of the Subscriber's face will be automatically compared with the Subscriber's photo from its identity document through the verifications under para. (2) or para. (3) below.

(2) Where it is technologically feasible, Evrotrust will perform an automated verification of the Subscriber's identity through a respective exchange of the data established under item 7.4.3.1 above with the registers of the primary data controllers in the respective country who issued the identity document, if such access is provided by the jurisdiction of the identity document issuing country.

(3) When using an identity document with an NFC chip, the identification will rely on data retrieved by means of an NFC chip on the Subscriber's identity document.

(4) Upon successful verification of the validity of the identity document and successful identification, it will be considered that the Subscriber has been successfully identified and its identity has been verified.

7.4.3.3. Semi-automated identification.

Upon unsuccessful automated identification, a mandatory verification and confirmation of the identification is required to be performed by an Evrotrust operator. In this case, a real-time videoconference call can be held through the mobile application between the Subscriber and an Evrotrust operator. Upon successful identification by the operator, the latter will confirm the Subscriber's identification and identity. If there are publicly available registers for verification of the validity of the identity document or the status of the person, such verification will be performed ex officio.

7.4.4. The video identification system for individuals used by Evrotrust is certified for compliance with the requirements of Regulation (EU) № 910/2014 by a conformity assessment body, which provides the same level of certainty as a personal appearance, pursuant to Art. 24, item 4 of Regulation (EU) № 910/2014 (also applicable to Evrotrust mobile application).

7.4.5. In order to ensure the highest possible level of security, mobile application „ID, operated by Evrotrust" does not support functionalities for the creation of security codes that require knowledge of the type of PIN code or secret word. Instead of using a PIN code, the access to the mobile application, as well as the activation/requesting of services in the mobile application (e.g. requesting the issuance of a QESQC, signing with a QESQC, etc.) and the confirmation of the execution of any legally valid electronic statements in or through the application, are confirmed through the functionalities for biometric data recognition (e.g. fingerprint, facial recognition, etc.) supported by the device used by the Subscriber. When using the functionalities for biometric data recognition supported by the device used by the Subscriber, the biometric data of the Subscriber remain under its control and are not stored by Evrotrust. Apart from the activities that require automated Subscriber identification (initial registration, account recovery when reinstalling the mobile application or provision of an electronic identification service with additional automated Subscriber identification in real time), Evrotrust does not process the Subscriber's biometric data. In the cases referred to above wherein Evrotrust processes biometric data, the processing will be one-time and Evrotrust will not store such data in its systems, but only the result of the processing performed (degree of matching).

7.4.6. Upon successful identification under item 7.4.3.2, Evrotrust will confirm the Subscriber's registration and send it the General Terms and Conditions, Terms of Use of Services Accessible through the "ID, operated by Evrotrust" Mobile Application, the applicable Personal Data Protection Policy and the Declaration of Consent for signing. These General Terms and Conditions are integral part of the Terms of Use of Services Accessible through the "ID, operated by Evrotrust" Mobile Application.

7.4.7. An obligatory condition for the successful completion of the registration and the use of the services is the issuance of a QESQC whereby the Subscriber shall sign the contract under the Terms of Use of Services Accessible through the "ID, operated by Evrotrust" Mobile Application and these General Terms and Conditions. For this purpose, the Subscriber shall requests, through the interface of the mobile application, the issuance of a QESQC by reviewing in advance the content of the data to be entered in the certificate and confirming its request for the issuance of a QESQC by:

(1) pressing the "Issue" button and

(2) confirming through biometrics, through a biometric data recognition functionality activated and supported by its device.

7.4.8. Evrotrust will issue the QESQC requested by the Subscriber through the functionalities of the Application. The Subscriber shall sign these General Terms and Conditions, the Terms of Use of Services Accessible through the „ID, operated by Evrotrust" Mobile Application, the applicable Privacy Policy and a Declaration of Consent. The signing through the issued QESQC will be activated through a biometric data recognition functionality available in the Subscriber's device. By signing those documents, it will be considered that the contract between Evrotrust and the Subscriber has been entered into. Prior to the signing of those documents, the issued QESQC may not be used for the signing of any other documents. If the Subscriber refuses to sign the General Terms and Conditions, the Terms of Use of Services Accessible through the „ID, operated by Evrotrust" Mobile Application, the applicable Privacy Policy and a Declaration of Consent, as well as in case the Subscriber fails to sign them before the expiry of the period

specified in its mobile application, the issued QESQC and the Subscriber's account will be deactivated, and its registration will be considered unsuccessful.

7.4.9. The contract signed by both the Subscriber and Evrotrust will be sent to the Subscriber via the mobile application. The wording of the contract (the General Terms and Conditions and the Terms of Use of Services Accessible through the "ID, operated by Evrotrust" Mobile Application) is available for storage on the Subscriber's device in a way that allows its download and storage on a local device, as well as subsequent reproduction in the "Account" menu of the application and on the Evrotrust's website. The Subscriber shall be obliged to store on its local device/send to its e-mail the signed contract/the General Terms and Conditions. The contract will be concluded in Bulgarian or in another language supported by the mobile application.

7.4.10. All identification data about the Subscriber collected in the process of its identification and registration, together with the 3D FaceMap (biometric identifier) generated in the automated identification by processing specific features of the Subscriber's facial image (biometric data) will be stored in a secure enclave on the Subscriber's device which is under the Subscriber's sole control. Evrotrust will in no way store the generated 3D FaceMap in its systems. Evrotrust will in no way have access to the secure enclave on the Subscriber's device.

7.5 QESQC

The issued QESQC requested through a mobile application will be published immediately after the contract has been signed in an Evrotrust certificate repository. If the Subscriber explicitly requests this, it may make a statement of will by activating the relevant functionality of the mobile application for control over the issued certificates, if any. The issued qualified certificate will have a period of validity depending on the policy applicable to the certificate in question, which shall commence from the date of its publication in the Evrotrust certificate repository.

7.6 CHANGE OF DEVICE

Evrotrust's mobile applications allow the Subscriber to add a new device:

a) Upon changing the device or adding a new device, the Subscriber shall identify itself with the e-mail address and PIN designated by it in the Evrotrust mobile application and by going through automated re-identification in the mobile application "ID, operated by Evrotrust";

b) The application may be used by the Subscriber through an unlimited number of devices. The Evrotrust system stores a list of all active devices through which the Subscriber uses the Application;

c) Each of the devices used by the Subscriber may be deactivated via the application, through the appropriate functionality.

8 SUBSCRIBER RIGHTS

8.1 RIGHT OF WITHDRAWAL

According to the consumer protection legislation currently applicable in the European Union, in cases where the Subscriber is a consumer within the meaning of the consumer protection legislation and the contract is concluded remotely or off-premises, it shall have the right, within 14 days from the date of conclusion thereof, without owing any compensation or penalty, and without stating a reason why, to withdraw from the contract. Such a contract is the contract concluded through a mobile application of Evrotrust. If the Subscriber wants to withdraw from the contract, it shall inform Evrotrust of its decision in writing before the expiry of the 14-day period from the conclusion of the contract. For the avoidance of doubt, it will be considered that the contract between Evrotrust and the Subscriber for the use of the services provided through the mobile application has been entered into from the time of signing the General Terms and Conditions by the Subscriber using the QESQC issued to it by Evrotrust. If the Subscriber wishes that the provision of the services commences before the expiry of the period for exercising the right of withdrawal, the Subscriber shall make an explicit request to this effect. In such cases, if the Subscriber exercises its right of withdrawal after having requested the commencement of the use of the services before the expiry of the period for exercising the right of withdrawal, it shall pay to Evrotrust the proportional amount of what has actually been provided to it up to the time when the Subscriber notified Evrotrust of the exercise of the right of withdrawal.

When issuing a short-term QESQC, insofar as the services are provided in full and immediately after the request with the acceptance of these General Terms and Conditions and with the request for the issuance of a short-term QESQC, the Subscriber expressly agrees and

confirms that it is aware that it will lose its right of withdrawal after having its requested short-term QESQC issued.

8.2 RIGHT OF ACCESS TO THE SERVICES

The Subscriber shall have the right to access the services subject to these General Terms and Conditions and the access requirements set by Evrotrust for each individual type of service.

9 SUBSCRIBER OBLIGATIONS

The Subscriber shall have the following obligations:

a) The Subscriber agrees to adhere to the terms and conditions set by Evrotrust in relation to the specifics of the services in terms of the type of provisioning regime, as well as in terms of any policy adopted by Evrotrust and designed to protect or improve the quality and reliability of the services;

b) The Subscriber shall by itself ensure the technical equipment, software, access to mobile telephone services and data transmission services over a mobile network necessary for its use of the services.

c) The Subscriber undertakes, when using the services, to:

- comply with the General Terms and Conditions, the contract and the applicable law;
- not to infringe foreign pecuniary or non-pecuniary rights, including intellectual property rights;
- immediately notify Evrotrust of any case of committed or detected violation in the use of the services;
- not to impersonate another person or otherwise mislead Evrotrust or third parties about its identity;
- provide correct, accurate and complete information required by Evrotrust in accordance with the General Terms and Conditions, the Policies and Practices and the applicable law, in its registration and identification, as well as in any other use of the application and/or the services;

- verify the completeness and accuracy of the content of the certificates issued to it and, in case of any discrepancy between the submitted information and the content of the respective certificate, immediately notify Evrotrust;
- discontinue using the mobile application, the services and the certificates issued to it in case of suspicion of any compromise of the PIN code, the manner of identification in the mobile application or in case of loss of its device with an Evrotrust application installed thereon or smart card/flash drive on which the certificate is issued, and immediately take actions for their cancellation/blocking/revocation with regard to Evrotrust;
- immediately notify Evrotrust in the event of any change in the information provided by it in relation to the use of the application and/or the services, as well as request immediate cancellation of the certificates issued in the event of any change in the information contained therein. When using a mobile application, the Subscriber shall, upon the occurrence of any change in the information provided by it, immediately update it through the relevant functionalities in the application. Upon any change in the information provided by the Subscriber in the application, the certificates requested and issued through the mobile application, which include data that has been updated, shall be automatically cancelled;
- use the mobile applications, the services, certificates issued by Evrotrust and the key pairs only for their intended purpose;
- not to commit any malicious acts.

d) The Subscriber shall take all care, take the necessary measures, in order to protect the means of identification in the mobile application, as well as to protect its devices. If, for example, the version of the mobile application requires a PIN code, it shall not make it available to third parties. The Subscriber shall be solely responsible for the protection of its PIN code and means of identification, as well as for all actions performed by it or by third parties through the use thereof;

e) The Subscriber/Signatory/Creator agrees that Evrotrust will process all data necessary for their successful identification and registration and for the verification of the data provided by the Subscriber, as well as any additional information necessary for the provision of the services, and will store it in accordance with these General Terms and Conditions, its applicable Privacy Policy and the applicable law. For the avoidance of doubt, such consent shall not constitute a consent to the processing of personal data within the meaning of Regulation (EU)

№ 679/2016, but rather a contractual consent. The applicable legal grounds on which Evrotrust processes personal data are described in detail in its applicable Privacy Policy.

10 EVROTRUST RIGHTS

a) Evrotrust, in its capacity as a qualified trust service provider, shall be entitled to:

- at its discretion and without giving a notice, suspend or temporarily restrict the Subscriber's access to the services if there is evidence or suspicion that the latter uses the same in violation of the applicable law or the General Terms and Conditions;
- require from the Subscriber and process all data necessary for the successful identification and registration of the Subscriber and for the verification of the data provided by the Subscriber, as well as any additional information necessary for the provision of the services;
- publish in its certificate repository all certificates issued by it in accordance with the requirements of the law and the Subscriber's instructions (as far as they are admissible).

b) Evrotrust shall not have the obligation and the objective possibility to control the method and/or the purposes for which the Subscriber uses the services provided, nor shall it be obliged to look for facts and circumstances indicating the performance of unlawful activities;

c) In the event of any breach by the Subscriber of any of the obligations provided for in Section 9 (c) above, Evrotrust shall have the right to terminate or suspend immediately and without notice the provision of the services or to terminate unilaterally and without notice the contract, as well as to notify the competent authorities in case of suspicion of any unlawful actions.

11 EVROTRUST OBLIGATIONS. SERVICE LEVEL (SLA)

11.1 EVROTRUST OBLIGATIONS

The obligations of Evrotrust shall include:

- to provide the services to the Subscriber in accordance with the General Terms and Conditions and the applicable law;
- to take immediate action in relation to the cancellation, renewal and revocation of certificates issued by it upon establishing the relevant grounds for this;
- to immediately notify the Subscriber of the circumstances regarding the validity or reliability of a certificate issued by it;

- to publish and update electronically a publicly available list of the certificates revoked by it;
- to carry out external audits at least every 2 years by independent auditors in order to verify the compliance of the trust service with the requirements of Regulation (EU) № 910/2014 and the applied policy.

Evrotrust warrants that it operates by:

1) strictly observing the terms and conditions referred to in this document, the requirements of Regulation (EU) № 910/2014, REGULATION (EU) 2016/679 and the applicable law in carrying out its activities as a qualified trust service provider;

2) its provided services not infringing any third party copyrights and license rights;

3) using technical equipment and technologies that ensure the reliability of the systems and the technical and cryptographic security in the implementation of the processes, including a secure and protected mechanism/device for the generation of keys and for the creation of an electronic signature/seal in its infrastructure;

4) issuing qualified electronic signature/seal certificates after verifying the information submitted by means permitted by law;

5) securely storing and keeping information related to the certificates issued and the systems operations;

6) observing the established operating procedures and rules for technical and physical control, in accordance with the terms and conditions in the Practice and Policy in the provision of qualified trust services;

7) upon request, issuing the relevant types of certificates, observing the conditions and procedures referred to in this document, the relevant Policies and Practices and generally adopted standards;

8) creating an opportunity for immediate cancellation and revocation of a qualified certificate;

9) cancelling and revoking certificates under the terms and conditions of the relevant Policies and Practices;

10) immediately notifying the interested persons (Relying Parties) after a certificate has been revoked;

11) providing conditions for the precise determination of the time of issuance, cancellation, renewal and revocation of the certificates;

12) performing procedures of identification and establishment of the authenticity of the Signatory /Creator;

13) ensuring measures against tampering of certificates and for the confidentiality of the data it has access to in the process of creating the signature/seal;

14) using reliable certificate storage and management systems;

15) allowing only duly authorized employees to have access for the purpose of making changes in the data, establishing the authenticity and validity of the certificates;

16) taking immediate measures in case of any technical problems related to security;

17) upon expiry of the period of validity of a qualified certificate, revoking its validity;

18) informing the Signatorys/Creators and the Relying Parties about their obligations and due care in the use of and relying on the trust services provided by Evrotrust, as well as about the correct and safe use of the issued certificates and the provided trust services related thereto;

19) using and storing the collected personal and other information only for the purposes of its activity of providing trust services in accordance with the applicable law;

20) not storing or copying any data of the creation of user private keys, unless it provides the remote signing service in accordance with Regulation (EU) № 910/2014;

21) keeping available funds which enable it to carry out its activities;

22) entering into an insurance for the time of its activities;

23) maintaining trusted personnel having the necessary expertise, experience and qualifications for carrying out the activities;

24) keeping a certificate repository wherein it publishes the issued qualified certificates

25) maintaining an up-to-date Certificate Revocation List (CRL);

26) publishing in its website other circumstances and electronic documents, according to this document and the applicable law;

27) providing protection against making changes to the certificate repository by unregulated and unlawful access or due to an accidental event;

28) immediately publishing in a certificate repository the issued and signed certificates;

29) performing periodic internal audits of the activities of the Certification Authority and the Registration Authority;

30) performing external audits by independent auditors and publishing on its website the results of such audits;

31) using in its activities certified software and hardware, as well as secure and reliable technological systems;

32) maintaining on Evrotrust's website a list of Registration Authorities, a list of recommended software and hardware for use by users, templates, forms, and other documents for the benefit of Subscribers.

Evrotrust shall be liable to the Signatory /Creator/Subscriber and the Relying Party for any damages caused by gross negligence or wilful intent:

a. resulting from failure to comply with the requirements of Regulation (EU) № 910/2014 in carrying out its activity of providing qualified trust services;

b. resulting from incorrect or missing data in the qualified certificate at the time of its issuance;

c. resulting from damages caused in case where at the time of issuing the certificate, the person designated as the Signatory /Creator did not have the private key corresponding to the public key;

d. resulting from the algorithmic discrepancy between the private key and the public key entered in the certificate.

e. resulting from failure to comply with its obligations to issue and manage qualified certificates;

f. resulting from failure to comply with the established policies for issuing a certificate in terms of establishment of the identity of the Signatory /Creator.

11.2 SERVICE LEVEL (SLA)

Evrotrust undertakes to:

(1) provide guaranteed time for recovery of an interrupted service within 48 (forty-eight) hours in working days. The period shall commence from the time of submitting an alert for

the existence of a problem, accepted and confirmed by Evrotrust.

(2) provide a guaranteed level of accessibility of the services for an annual period equal to 98%. Accessibility represents the total time within the calendar year during which the Subscriber is able to use the services upon the existence of its agreed parameters. Such accessibility parameter value shall not include the scheduled technical maintenance, or interruptions beyond the control of Evrotrust.

(3) provide technical support of the services 24 (twenty-four) hours a day, 365 days a year, by registering and eliminating any technical problems within the technological time for their servicing.

(4) monitor the proper functioning of the services in order to ensure their continuity.

(5) In case of breach of security or breach of integrity, which have a significant impact on the provided trust service or on the stored personal data, Evrotrust shall notify thereof without undue delay, but in any case within 24 hours from the time when it became aware of the occurrence of the event, the supervisory authority and, where applicable, other competent authorities, such as the competent national information security authority or the data protection authority. Where a breach of security or breach of integrity is likely to adversely affect a Subscriber, Evrotrust shall also notify, without undue delay, the person concerned of the breach of security or breach of integrity.

(6) Evrotrust has developed a procedure for filing, reviewing and resolving complaints and claims, through which Evrotrust serves its Subscribers.

(7) The level of service (SLA) described herein applies only to Service Subscribers with whom no individual contract has been entered into which may specify specific parameters for the level of service other than those described.

(8) The service level (SLA) described herein applies only to services that the Subscriber uses and for which the Subscriber pays.

12 SUBSCRIBER RESPONSIBILITY

The Subscriber's responsibilities shall include:

1) The Subscriber shall be responsible for fulfilling the obligations provided for in these General Terms and Conditions;

2) The Subscriber shall be solely responsible for the use of its PIN code or other means of identification, as well as for any use by third parties allowed by it. The Subscriber shall be solely responsible for the protection of its devices with mobile applications of Evrotrust installed thereon and for any use thereof allowed by it;

3) The Subscriber shall indemnify Evrotrust for any suffered damages and lost profits, including for paid pecuniary sanctions, paid attorney's fees and other expenses, as a result of claims brought by, and/or compensations paid to, third parties in relation to a breach by the Subscriber of its obligations provided for in the General Terms and Conditions, the Policies and Practices and any other documents that form an integral part of the contract, as well as for damages caused by failure by the Subscriber to perform its obligations under the applicable law.

4) The Subscriber represents and agrees that Evrotrust will not be liable for any damages caused to the Subscriber in the use of the mobile applications of Evrotrust and Evrotrust services, unless they are caused by Evrotrust by wilful intent or by gross negligence or if a legal act explicitly provides otherwise.

5) The Signatory /Creator shall be liable to Evrotrust and all Relying Parties if:

(a) in the creation of the private-public key pair, it has used an algorithm and electronic signature/seal creation devices that do not meet the requirements of Regulation (EU) № 910/2014;

(b) it does not exactly comply with the security requirements set by Evrotrust;

(c) it does not require from Evrotrust to cancel or revoke the certificate after becoming to know that the private key was misused or is threatened of being misused, including, but not limited to, in the event of loss or theft of the flash drive/the smart card on which the certificate is issued, or of a device on which a mobile application of Evrotrust is installed, or the PIN code or other means for identification becoming known by or available to unauthorized third parties;

(d) it has made false statements before Evrotrust which are also relevant to the content or the issuance of the qualified certificate;

(e) where the certificate was issued with a stated Creator and a person authorized by it, it shall be liable for the failure by such authorized person to fulfil its obligations.

6) The Subscriber, the Signatory /Creator or the authorized representative of a legal entity shall be responsible for the content of the attached files and the consequences of their use.

7) The Signatory/Creator shall be liable to Evrotrust if it or its authorized person has provided incorrect data, respectively has concealed data related to the content or the issuance of the certificate, as well as when it has not properly stored the private key corresponding to the public key stated in the certificate;

8) The Signatory/Creator shall be solely responsible for the protection of the private key after providing the data for activation of the smart card (in the case of issuance of a certificate on a flash drive/smart card).

13 LIABILITY AND LIMITATION OF LIABILITY

13.1. Evrotrust, as a qualified trust service provider, shall be liable:

a) under Art. 13 of Regulation (EU) № 910/2014, as well as under the applicable law, for damages caused by wilful intent or by gross negligence on third Relying Party individuals or legal entities that are not parties to a contract with it;

b) under Art. 13 of Regulation (EU) № 910/2014, as well as under the applicable law, for damages caused by wilful intent or by gross negligence on the Subscriber;

c) Evrotrust shall not be liable to the Subscriber for any damages resulting from incorrect, incomplete or inaccurate data provided by the Subscriber;

d) Evrotrust shall not be liable for any damages caused:

- on the software, hardware, the device or other telecommunication equipment, or for loss of data resulting from materials or resources sought, loaded or used in any way whatsoever through the services provided;
- as a result of an untimely request by or failure by the Subscriber to require the suspension/blocking/termination of a mobile application, services and/or the certificates issued to the Subscriber;
- as a result of failure by the Subscriber to perform any of its obligations as provided in the General Terms and Conditions or in any other documents forming an integral part of the contract, as well as for damages caused by failure by the Subscriber to perform any of its obligations according to the applicable Evrotrust Policies and Practices or the applicable law;
- as a result of the use of a certificate beyond the limits of its intended purposes and the restrictions on its validity as stated therein.

e) Evrotrust shall not be responsible for the availability and quality of any goods and/or the content of services provided to the Subscriber by third parties, including Relying Parties. Insofar as the actions of such third parties are not under the control of Evrotrust, the latter shall not be responsible for the unlawful nature of the activities of such third parties or for the emergence, warranty, performance, amendment and termination of obligations and commitments undertaken in relation to goods or services offered by such third parties, and shall not be liable for any damages and lost profits arising from such relationships.

f) Evrotrust shall not be responsible for the non-provision of the services upon the occurrence of circumstances beyond its control - force majeure events, accidental events, problems in the global Internet network or in the electronic communications networks or in the provision of services beyond the control of Evrotrust, as well as in case of unregulated access or intervention by third parties in the operation of Evrotrust's mobile applications through the Subscriber's device;

g) Evrotrust shall not be liable to the Subscriber or third parties for any damages suffered and lost profits incurred as a result of the termination, suspension, change or limitation of the services.

h) The Parties agree that Evrotrust shall not be responsible for the non-provision or deterioration of the services as a result of tests or maintenance performed by Evrotrust for the purpose of inspecting equipment, connections, networks, etc., as well as tests aimed at improving or optimizing the provided services. In such cases, Evrotrust shall notify the Subscriber in advance of any possible temporary non-provision of the services, respectively of their deterioration, by sending an IM message or a short text message (SMS) or an e-mail to the registered e-mail.

13.2. Evrotrust shall not be liable in cases where the damages occurred are the result of failure to take due care, failure to fulfill any obligations or lack of knowledge in the field of PKI (Public Key Infrastructure) technologies by Subscribers or Relying Parties.

13.3. Evrotrust shall further not be liable in cases of damages caused by:

➢ the use of a certificate beyond the limits of its intended purposes and restricted effect stated therein, with regard to the purposes for use and the limitation on the value of the transactions;

➢ illegal actions by Subscribers or Relying Parties;

➢ provision by the Signatory /Creator of the means of identification on the signature/seal creation device and access to the private key to third parties;

➢ accidental events having a force majeure nature, including malicious acts of third parties (hacker attacks, seizure of the signature/seal creation device, access to the private key, the means of identification becoming known without the knowledge of the Signatory, etc.);

➢ use of a certificate that was not issued or used in accordance with the requirements and procedures of the Evrotrust Practice and Policy;

➢ use of an invalid certificate (a certificate that has been cancelled or revoked);

➢ untimely act of revocation or cancellation of a certificate (the consequence of a request delayed by the Signatory /Creator or due to reasons beyond the control of Evrotrust);

➢ compromised private key corresponding to the public key in the certificate due to the fault of the Signatory /Creator;

➢ poor quality and functionality of the software products and hardware devices used by the Signatory /Creator and Relying Parties.

13.4. The compulsory insurance shall cover the liability of Evrotrust to Signatory s/Creators, respectively Relying Parties, for pecuniary and non-pecuniary damages caused up to the limits determined in the applicable law. Upon the occurrence of an event that may allow for a claim to be brought that is covered by the insurance, the affected person shall notify in writing Evrotrust and the Insurer within 7 days after becoming aware of the event. The insurance coverage for non-pecuniary and/or pecuniary damages caused to the Signatory /Creator shall not exceed the amount established by the applicable law. The liability, respectively the insurance, shall not cover any damages caused by:

➢ failure by a Signatory /Creator to fulfil its obligations;

➢ compromise or loss of a private key of a Signatory /Creator due to failure to take due care to protect the key during use;

➢ failure by the Relying Party to comply with the requirements for verification of the validity of the electronic signature/seal and the qualified certificate;

➢ force majeure and other circumstances beyond the control of Evrotrust.

14 PRICES

Evrotrust has determined the following method of payment by Subscribers for the provision of trust services:

a) Evrotrust provides the services either free of charge or for a fee, in accordance with the prices specified in the tariff for the use of the services accessible through the Evrotrust application (the Tariff). The Tariff is available in the mobile applications and at Evrotrust's website;

b) Evrotrust reserves the right to unilaterally change the prices announced in the Tariff, subject to the requirements of the applicable law. The change in prices shall not affect the use of services already paid for by the Subscriber;

c) The prices for the use of the services shall be paid to Evrotrust by the Subscriber or by the Relying Party according to the arrangements between them;

d) The prices for the use of the services shall be due as provided for in the Tariff:

- for each individual use of a service; or
- in another way as specified in the Tariff.

e) Where the price for a given service is due by the Subscriber, the mobile application will display accurate information about its value along with all due taxes and other expenses and an indication of when the obligation to pay it arises;

f) Payment by the Subscriber for the services may be made:

- through the "Portfolio" service on the App Store or Google Play;
- as a value-added service of the mobile operator which the Subscriber has subscribed with, with the value of the services used by the Subscriber being included in the monthly invoice of the Subscriber issued by the mobile operator for the relevant month;
- by crediting by direct debit of the Subscriber's payment account with its prior consent, where Evrotrust has integration with the relevant payment service provider; or
- in another way established by Evrotrust.

14.1 PORTFOLIO

Evrotrust provides the following "Portfolio" service to Subscribers:

a) The "Portfolio" service on the App Store and Google Play provides the Subscriber with the opportunity to pay the cost of the paid services used on a subscription basis;

b) The Subscriber may subscribe through its Portfolio to a specific plan including a certain number of signatures per month, with the amounts thereunder being paid monthly;

c) According to the functionality provided in the mobile application, when the number of signatures or other trust services covered by the subscription is exhausted, the Subscriber may switch to another plan, otherwise it shall wait until the next subscription period.

15 AMENDMENT AND TERMINATION

15.1 AMENDMENT OF THE GENERAL TERMS AND CONDITIONS

Evrotrust allows amendments to the General Terms and Conditions in the following cases:

a) Evrotrust may unilaterally amend the General Terms and Conditions, notifying the Subscriber of any amendment in accordance with the requirements of the law;

b) Where it does not agree with the amendments, the Subscriber may withdraw from the contract without stating any reason therefor and without owing any compensation or penalty. In such case, the contract shall be automatically terminated upon receipt by Evrotrust of the Subscriber's notice under item 15.1 (c), unless Evrotrust has explicitly indicated the possibility to continue using the Services under the terms and conditions applicable before the amendment. This rule shall not apply in cases where the amendment to the terms of the General Terms and Conditions is due to an order or instruction of a competent authority;

c) The Subscriber may exercise its right under item 15.1 (b) by a respective statement addressed to Evrotrust within one month from the notice under item 15.1 (a). If within the said period the Subscriber does not declare that it does not agree with the amendments, it will be deemed to be bound by them.

15.2 TERMINATION OF THE CONTRACT

Evrotrust allows the termination of a contract with a Subscriber in any of the following cases:

a) Except in the cases provided for in these General Terms and Conditions, it shall also be terminated upon:

- suspension of the activities or termination of Evrotrust;
- termination of the support of a mobile application used by the Subscriber;
- deletion of the Subscriber's account from the mobile application used by the Subscriber;

- mutual consent of the parties; or
- in other cases provided by law or agreed between the parties.

b) The Subscriber shall have the right, at any time, at its own discretion, to stop using the services. The Subscriber may unilaterally terminate the contract by deleting the Evrotrust application installed on its device or by requesting the revocation of the certificates issued to it. In case the application is used by the Subscriber on several devices, then the deletion of the application on one of those devices shall not terminate the contract, unless the Subscriber has deleted its account;

c) The Subscriber shall be considered to have been informed and agrees that all electronic statements made until the termination or cancellation of the contract will be automatically sent through the application and it is not possible to revoke or cancel them regardless of the subsequent termination or cancellation of the contract.

15.3 MANAGEMENT OF STORED DOCUMENTS AFTER TERMINATION OF THE CONTRACT

Evrotrust manages and stores documents under the following conditions:

a) (only applicable to Evrotrust mobile application) Evrotrust stores in a secure environment, in encrypted form, all documents signed by the Subscriber through services accessible in a Evrotrust mobile application within the period agreed with the Subscriber - 10 years, in a way that provides the Subscriber with access to them. All documents that are served on the Subscriber through the qualified delivery service are stored ("electronic registered delivery" within the meaning of Regulation (EU) № 910/2014) in the same way. The stated documents will be stored by Evrotrust until they are deleted by the Subscriber or until the termination of its contract, but not longer than the period agreed with it. The service will only be available as long as the Subscriber has an active account in the mobile application;

b) The deletion of documents shall not lead to the deletion of information intended to provide evidence of the sending, receipt and signing of documents through the mobile application.

16 PERSONAL DATA PROTECTION

16.1 PERSONAL DATA PROCESSING

Evrotrust carries out its activity of provision of trust services in accordance with the

requirements of REGULATION (EU) № 2016/679 (GDRP), the applicable law and in accordance with its applicable Privacy Policies which form an integral part of these General Terms and Conditions and the contract with the Subscriber.

The applicable Privacy Policies of Evrotrust include:

1. Privacy Policy Applicable to the Trust, Information, Cryptographic and Other Services Provided by „Evrotrust Technologies" AD (all services);

2. Privacy Policy Applicable to the provision of Services through Evrotrust Mobile Application;

3. Privacy Policy Applicable to the Mobile Application "ID, operated by Evrotrust"; and

4. Other privacy policies which Evrotrust may adopt and apply with regard to the provision of some of its services.

The Privacy Policy Applicable to the Trust, Information, Cryptographic and Other Services Provided by „Evrotrust Technologies" AD (specified above under item 1) is applicable to the activities carried out by Evrotrust in the provision of services subject to these 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 when providing these services. In the event of a conflict between the Privacy Policy Applicable to the Trust, Information, Cryptographic and Other Services Provided by „Evrotrust Technologies" AD 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 the Privacy Policy Applicable to the Trust, Information, Cryptographic and Other Services Provided by „Evrotrust Technologies" AD shall apply.

Prior to the conclusion of the contract, the Subscriber shall get acquainted with the Personal Data Protection Policy applicable to the services requested by the Subscriber in order to find out in what way, what type of personal data and for what purposes are is processed by Evrotrust, as well as to be informed about their rights and all other important issues concerning the protection of their personal data in accordance with the GDPR.

The provision of the services is inherently related to the receipt, transfer, storage, transmission and processing of Subscriber data through the Evrotrust system to Relying Parties,

as well as the exchange of such data between them and Evrotrust in accordance with the applicable law and the established contractual relations between all the above persons. The Subscriber shall be considered to have been informed about the above and agrees that their data will be provided to third parties for the purposes of providing the services.

16.2 DATA PROTECTION OFFICER

Evrotrust has appointed a Data Protection Officer (DPO) within the meaning of Art. 37-39 of Regulation (EU) 2016/679. The DPO shall be the point of contact for Subscribers in connection with the exercise of their rights under the Evrotrust Personal Data Protection Policies and the applicable personal data protection legislation relating to their personal data processed by Evrotrust.

Contact address:

Sofia, 1766, "Okolovrasten pat" 251G, Business center MM, floor 5

e-mail: dpo@evrotrust.com

17 FILING COMPLAINTS AND DISPUTE RESOLUTION

17.1. Procedure before Evrotrust

Any disputes arising out of or relating to a contract entered into under these General Terms and Conditions, including disputes arising out of or relating to the interpretation, invalidity, non-performance or termination of the contractual relationship, will be resolved by mutual agreement between Evrotrust and the Subscriber. Complaints regarding the use of certificates and trust services provided by Evrotrust will be reviewed by Evrotrust after written information has been submitted to:

Evrotrust Technologies AD

Sofia, 1766

„Okolovrasten pat“ 251G, Business center MM, floor 5

Telephone/Fax: + 359 2 448 58 58

In carrying out this procedure, the complainant will receive a reply within 1 (one) month after receipt of the complaint, except in cases where the applicable law explicitly provides for another period for reply.

17.2. Exceptions to the procedure before Evrotrust under 17.1

The above period and the above procedure shall not apply to disputes, complaints and requests related to the processing of personal data. Such requests shall be dealt with in accordance with the applicable Personal Data Protection Policy of Evrotrust and in accordance with the periods and requirements of Regulation (EU) № 2016/679 and the applicable law.

17.3. The European Commission keeps an out-of-court online dispute resolution platform, which is available at the following web address: www.ec.europa.eu/consumers/odr. On this platform, users can find a list of ADR bodies that can assist in out-of-court/alternative dispute resolution. Evrotrust does not wish and is not obliged to participate in dispute resolution procedures before ADR bodies, unless such an obligation is explicitly provided for in the applicable law or Evrotrust has given its explicit consent to participate in such a procedure.

17.4. In-court dispute resolution

If no agreement has been reached between the parties, the dispute will be referred for resolution to the relevant Bulgarian court of competent jurisdiction. When the subject of the dispute between the parties is property rights, it will be referred for resolution to a competent court based in Sofia City.

18 POLICIES AND PRACTICES APPLICABLE TO THE TRUST SERVICES PROVIDED BY EVROTRUST

In accordance with the requirements of Regulation (EU) № 910/2014, Evrotrust includes in the issued certificates an object identifier (OID)/link (URI), through which Subscribers are able to check the Evrotrust Policies and Practices applicable to the provision of the trust service related to the issued certificate. Each of the Evrotrust Services is provided in accordance with the Policies and Practices applicable thereto. The Policies and Practices applicable to the trust services provided by Evrotrust are publicly accessible on the website of Evrotrust: https://www.evrotrust.com/. Each version of the Practice for providing a qualified trust service will be applied until the approval and publication of a new version. The Subscribers and Relying Parties shall be obliged to get acquainted in advance with and to comply only with the valid version of the Policies and Practices applicable at the time of using the Evrotrust services.

19 ACCESSIBILITY. LOGS. AUDIT/CONFORMITY ASSESSMENT

19.1 CONFORMITY ASSESSMENT

Evrotrust is audited at least once every 24 months by a conformity assessment body accredited by the European Commission. The purpose of the audit is to confirm that Evrotrust, as a qualified trust service provider, and the qualified trust services it provides, meet the requirements set out in EU Regulation № 910/2014.

19.2 AVAILABILITY

Evrotrust ensures that the availability of the services is in accordance with the terms and conditions described in its Policies and Practices and in these General Terms and Conditions. Evrotrust provides uninterrupted access (24/7/365) to remote services and support services, with the exception of technical maintenance time.

19.3 LOGS

Evrotrust stores in logs events that are needed as evidence. Evrotrust collects the following information:

a) System logs: This includes records of the operation of the system, collected from the support services and tools of the operating system. These logs are kept for at least 1 (one) year;

b) Audit logs (Security): These are a set of chronological records related to security that provide documentary evidence of the sequence of activities that affected an operation, procedure or event. These records are kept for at least 1 (one) year;

c) Application logs: These are records containing information about events that occurred within a software application. This information is retrieved from the application and includes errors, warnings, and information events. These records are kept for at least 1 (one) year.

Evrotrust records the exact time of events important for the activity management, such as key management, clock synchronization, events related to identification of persons, issuance of certificates and others. Events are recorded in a way that cannot be easily deleted or destroyed, unless they are reliably transferred to long-term backups within the period in which they must be kept.

20 OTHER PROVISIONS

20.1 DEFINITIONS

In enforcing and interpreting the Contract, the terms used will have the following meanings:

a) **Evrotrust Technologies AD (Evrotrust)** is a joint stock company with UIC 203397356, having its registered office and business address at: 1113 Sofia City, Izgrev Region, Iztok Residential District, 2 Nikolay Haytov Str., entrance 5, 2nd floor, correspondence address: Sofia, 1766 "Okolovrasten pat" 251G, Business center MM, floor 5, tel. (+359 2) 448 58 58, e-mail: office@evrotrust.com, website: https://www.evrotrust.com/, as a qualified and unqualified trust service provider entered in the Trusted List of Qualified Trust Service Providers kept by the Communications Regulation Commission;

b) **Information system (system)** is any individual device or set of interconnected or similar devices, which in the execution of a certain program provides, or one of the elements of which provides, automatic data processing;

c) **Devices** are hardware products or parts thereof intended to connect to the interfaces of public electronic communications networks. The devices through which the services can normally be used are mobile phones or other smart devices that meet the technical requirements for normal installation and operation on an mobile application of Evrotrust;

d) **mobile application** is software installed on the Subscriber's smart device which enables the use of the services;

e) **Malicious acts** are actions or inactions that violate Internet ethics or harm individuals connected to the Internet or associated networks, sending unsolicited messages (unsolicited commercial messages, SPAM, JUNK MAIL), channel overflow (FLOOD), gaining access to resources with foreign rights and passwords, taking advantage of deficiencies in information systems for own benefit or information retrieval (HACK), change of identity, performing actions that may qualify as industrial espionage or sabotage, damage or destruction of information systems or information arrays (CRACK), sending "Trojans" or causing the installation of viruses or remote control systems, disrupting the normal operation of other users of the Internet and associated networks, performing any actions that may qualify as an offense or violation under the applicable law.

f) **Accidental event** is an event or action unforeseen and unpredictable at the time of the conclusion of the contract, wherein there is no culpable conduct by Evrotrust and which renders impossible the provision of the services.

g)**Server** is a device or system of connected devices on which, or on any of which, system software is installed for the performance of tasks related to the storage, processing, reception or transmission of information.

h)**PIN code** is a code that is generated by the Subscriber and entered by it at each launch of the Evrotrust mobile application and which, in combination with other data, serves to identify the Subscriber before the Subscriber's application for remote access to its private keys;

i) **Electronic signature, electronic document, electronic identification, trust services, electronic seal, qualified electronic signature certificate, advanced electronic signature, qualified electronic registered delivery service, and all other terms used in the Contract** shall have the meanings given to them in the relevant applicable regulations such as, but not limited to, Regulation (EU) № 910/2014, the Bulgarian Electronic Document and Electronic Trust services Act and the Bulgarian Electronic Identification Act, unless explicitly provided otherwise in the Contract;

j) **IM (Instant Messaging) messages** are encrypted messages that the Evrotrust application sends to or receives through the Evrotrust information system (the system).

20.2 INTELLECTUAL PROPERTY RIGHTS

The relations between Evrotrust and Subscribers with regard to intellectual property rights shall be settled as follows:

a) The intellectual property rights over mobile applications and over all other software applications and products, databases and other materials and resources in relation to the provision of the services shall be subject to protection under the Bulgarian Copyright and Related Rights Act, shall belong to Evrotrust or to the designated person who has transferred its right to use to Evrotrust, and may not be used in violation of the applicable law;

b) The Subscriber's right of access to the services shall not include the right to copy or reproduce information and to use intellectual property objects, unless it is a matter of information negligible in its volume which is intended for personal use, provided that this does not unduly harm the legitimate interests of the authors or other Signatorys of intellectual property

rights, and in the event that such copying or reproduction is carried out for non-commercial purposes. Notwithstanding the above, the Subscriber shall not be entitled to remove the trademark and other intellectual property right marks from the materials it is provided access to, regardless of whether the Signatory of those rights is Evrotrust or a third party.

20.3 WRITTEN FORM

The written form shall be considered to have been complied with by sending an IM message, a short text message (SMS), an e-mail message, a message in a mobile application of Evrotrust, pressing a virtual button in a mobile application of Evrotrust or marking a field (marking the relevant functionality) in the mobile application and the like, insofar as the statement is technically recorded in a way that allows its reproduction.

20.4 INVALIDITY

The Parties declare that in the event that any of the clauses of this Contract is held to be invalid, this will not entail the invalidity of the Contract, other clauses or parts thereof. The invalid clause will be replaced by the mandatory norms of the law or the established practice.

20.5 APPLICABLE LAW

The provisions of the legislation applicable in the Republic of Bulgaria shall apply to any issues not settled by the contract. The UN Convention on Contracts for the International Sale of Goods shall not apply. If the Subscriber is a consumer within the meaning of the applicable consumer protection legislation and is established on the territory of a country other than the Republic of Bulgaria, the enforcement of mandatory legal norms in that country, for which no derogation is allowed and which are intended to protect the rights of consumers, shall not be affected by the choice of applicable law in this Section.

21 REFERENCES

This document has been developed in accordance with the European and national legislation:

a) Regulation (EU) № 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[1];

b) 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[2];

c) Electronic Document and Electronic Trust services Act[3];

d) Electronic Identification Act[4];

e) Electronic Government Act[5].

21.1 PUBLICATION OF INFORMATION

Evrotrust publishes the following information on its website: https://www.evrotrust.com:

- The terms and conditions for the issuance, use and revocation of a qualified certificate, including the rules for identification/authentication;
- Security procedures for issuing and managing certificates;
- Conditions for access to a certificate and means of verification of a qualified certificate;
- Tariff for trust, information, cryptographic and consultancy services provided;
- List of types of devices compatible with the Evrotrust application;
- Information on the versions of the Evrotrust application, with the possibility for their direct download and installation;
- Policies and Practices for providing qualified trust services;
- Instructions on any other relevant technical requirements for the use of the services;
- Additional information about the services, their current scope, communications and notices.

[1] *https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:32014R0910*
[2] *https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=celex%3A32016R0679*
[3] *https://www.lex.bg/laws/ldoc/2135180800*
[4] *https://www.lex.bg/bg/laws/ldoc/2136822116*
[5] *https://www.lex.bg/laws/ldoc/2135555445*

This document is published on the Evrotrust website in the Bulgarian and English languages. In case of any discrepancy between the Bulgarian and English texts, the Bulgarian text shall prevail.