V. 4.0/ 15.04.2022

№ ……..

Today, ……, in the city of Sofia, between:
1. EVROTRUST TECHNOLOGIES JSC, registered under UIC: 203397356, address: city of Sofia, Iztok Quarter, 2 Nikolay Haytov St, entr. 5, fl. 2, bank account: IBAN: BG81UNCR70001522194489, BIC: UNCRBGSF, Unicredit Bulbank AD, city of Sofia, represented by the executive director Konstantin Bezuhanov, through …… proxy, hereinafter referred to as Qualified Provider of Certification Services (**PROVIDER**) within the meaning of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and certification services for electronic transactions in the internal market and repealing Directive 1999/93/EC (The Regulation)
and
2. ……, PIN ……., permanent address:
……., telephone …… , e-mail address:
…… ,

hereinafter referred to as **CLIENT**, on the other hand,

on the ground of the "Practice for providing qualified certification service" of the PROVIDER, the Regulation and the standards related to it, and the applicable European Legislation, as well as the regulatory framework in force in the Republic of Bulgaria, the present contract was signed for the following:

I. SUBJECT OF THE CONTRACT

Art. 1.
The PROVIDER shall provide to the CLIENT, in return for payment, certification services for the issuance, maintenance and management of certificates for qualified/advanced electronic signature/seal or website authentication (hereinafter referred to as qualified certificates) and other certification, information, cryptographic and consulting services. The requested qualified certificates and other certification services shall be specified in the requests for providing certification services to the present contract.

II. DURATION OF THE CONTRACT

Art. 2.
1. This contract was signed for a period until expiry of the validity term of the last qualified certificate and, in the event that the CLIENT is using certification, information, cryptographic or consulting services – until expiry of their validity or termination of their use.
2. The term shall begin on the date of the publishing of the first qualified certificate in the public register of the PROVIDER or at the start of the use of another certification, information, cryptographic or consulting service.

III. RIGHTS AND OBLIGATIONS OF THE PARTIES

Art. 3. The PROVIDER shall:

1. inform the CLIENT about the terms and conditions for issuance and usage of qualified certificates, including the restrictions on their effect, as well as the procedures for the submission of complaints and for dispute resolution;
2. issue qualified certificates to the CLIENT and publish them immediately;
3. not store and copy data for creating private keys;
4. undertake actions in relation to the suspension, renewal and termination of the effect of qualified certificates after establishing the respective grounds for them;
5. publish and update electronically a publicly available list of terminated qualified certificates
6. fulfill all of its obligations provided in the applicable policies and practices of the PROVIDER;
7. keep the agreement signed with the CLIENT for a period of at least 10 years.

Art.4.

The PROVIDER shall be entitled to:

1. request from the CLIENT supplementary information when issuing qualified certificates with the goal to identify the CLIENT and verify the data provided when processing the request to provide certification services, as well as to collect automatically, pursuant to the Law on Electronic Management, any data about the CLIENT from the primary data administrators;
2. terminate and stop the qualified certificates of the CLIENT, according to the terms and conditions established in the PROVIDER's applicable policies and practices.

Art.5

By signing this contract, the PROVIDER represents and warrants that each qualified certificate with a specified identifier (OID) of a Policy (CP) shall be issued in accordance with the applicable policies and practices of the PROVIDER.

Art.6

The CLIENT shall:

1. pay the PROVIDER the agreed remuneration, formed according to the requests for providing certification services hereto;
2. store/keep the private keys during the entire validity period of the qualified certificates in a manner that protects them against their compromising, loss, disclosure, modification and unauthorized use.
3. when the PROVIDER provides the CLIENT with a secure cryptographic device, the CLIENT shall use it and change its access PIN code before using the qualified certificate related to it;
4. provide the PROVIDER with true and complete information requested according to the requests to provide certification services;
5. accept the content of the qualified certificates issued under the contract and, within 3 (three) days from the issuance and publishing of the qualified certificate, the CLIENT shall check its content for correctness and, in the event of a discrepancy between the information provided and the content of the qualified certificate, the CLIENT shall inform the PROVIDER immediately;
6. immediately request from the PROVIDER to stop or terminate a qualified certificate in all cases described in the PROVIDER's applicable policies and practices, including in the event of changes in the information contained in the issued qualified certificate;
7. inform the PROVIDER about any changes in the information not included in an issued qualified

certificate, but provided according to the specified requirements on the information in the requests to provide certification services;
8. use the issued qualified certificates only as intended, in accordance with the applicable legislation and according to the applicable policy of the PROVIDER, as well as comply with all other conditions, requirements and obligations specified in the applicable practices derived from the respective policy for the provision of certification services for the respective type of qualified certificate;
9. stop using a certificate and the associated private key and duly request the certifying body to terminate a certificate in the event that: (a) any information or part of it is or shall become incorrect or imprecise, or (b) if there exists any real usage or suspicions for incorrect usage of the private key associated with the public key embedded in the certificate;
10. stop using the private key associated with the public key embedded in a certificate upon termination of such certificate by the PROVIDER;
11. follow the instructions by the PROVIDER related to compromising the private key or incorrect usage of a certificate, as soon as possible.

Art.7
The CLIENT shall be responsible
1. for generating a pair of keys, if the pair is created by him, whose private key shall be certified in the qualified certificates issued hereunder;
2. for the secrecy and integrity of the private key, from the moment of the creation of cryptographic key pairs, if they are created by the CLIENT;
3. for the use of the private key. The PROVIDER shall not bear responsibility for the usage of the cryptographic key pairs. Each use of a cryptographic private key shall be understood as action on the part of the CLIENT.

Art. 8.
By signing this contract, the CLIENT declares that:
1. the CLIENT has received, is completely knowledgeable of, accepts and assumes the obligation to comply with the applicable practices and policies for the requested qualified certificates and certification, information, cryptographic and consulting services by the PROVIDER;
2. the CLIENT was informed of the qualified status of the PROVIDER;
3. was informed by the PROVIDER of the terms and conditions for the issuance and usage of qualified certificates, including the restrictions on their effect, as well as of the procedures for submittal of complaints and dispute resolution;
4. is familiar with the requirements related to the use of qualified electronic signature/seal certificate provided in the Regulation and related standards;
5. during the remote generation of the private-public key pair, the technical means, software, communication and procedures used by the CLIENT shall be sufficiently secure and reliable and, in the event that their security is compromised, the CLIENT shall inform the PROVIDER immediately;
6. the entire information provided to the PROVIDER in the process of issuance of a qualified certificate, as well as the information contained herein, is true, accurate and complete and the CLIENT shall inform the PROVIDER promptly in the event of any changes in the information provided or the one contained in the issued qualified certificates;
7. the private keys that are under the CLIENT's control and which correspond to their public key

and are technically suitable according to the applicable policies and practices of the PROVIDER;
8. give his consent to the PROVIDER to collect, store and process his personal data and declares that he is informed that: the PROVIDER shall use them for the needs of its activity as a qualified provider of certification, information, cryptographic and consulting services; shall process and store them electronically and on paper; the provision of the personal data specified in the Regulation and the related standards and the applicable legislation is obligatory, the provision of any personal data outside of the framework of the activity of the PROVIDER under the Regulation and related standards and the applicable law is voluntary, and the refusal to provide personal data shall be ground for not concluding the contract or for its termination; recipients who can receive the data are the persons established by law; the access to the personal data for requesting changes shall be realized through the PROVIDER at the address provided on its Internet page http://www.Evrotrust.com;
9. the CLIENT is familiar and agrees with the applicable practices and policies, the General Terms and Conditions of the contract for certification, information, cryptographic and consulting services, the Price Schedule for the provided certification, information, cryptographic and consulting services, Statement on the infrastructure of the public key (PKI Disclosure statement/PDS) and the remaining public documents published on Evrotrust's site, related to the provided service;
10. is informed and agrees that the PROVIDER shall keep records of the information used at registration, the manner of provision of the device and each subsequent termination, third party identification attributes, and other specific data included in the certificates. The transmission of the information to third parties shall be realized under the terms and conditions required in the applicable policy and practice of the PROVIDER, in the event that the latter terminates its services;
11. is informed and consents the PROVIDER to publish the CLIENT's certificates in accordance with Evrotrust's applicable policies and practices;
12. the information contained in the certificates is correct;
13. the Client is familiar with the limits of Evrotrust's responsibility;
14. is informed of and gives its consent to the Evrotrust to terminate a certificate immediately, if the terms and conditions of use have been violated or if it is found that a certificate was used for criminal or other actions contrary to internet ethics, such as phishing attacks, faming, fraud, dissemination of malware, etc.

IV. PRICES AND PAYMENT METHOD

Art. 9.

1. The remuneration for the issuance and use of qualified certificates of the CLIENT and for the requested services shall be determined pursuant to the requests for provision of certification services hereto, according to the services listed in the PROVIDER's price schedule.
2. The payment of the amounts due shall be done by bank transfer to the PROVIDER's bank account specified herein or by using other electronic payment methods provided by the PROVIDER.
3. For the payment of any amounts due hereunder, the payment date shall be the date on which the PROVIDER's account reflected the transaction.
4. The remuneration for the issuance to the CLIENT and usage of qualified certificates and for the requested services shall be paid before the issuance of the qualified certificates and before using the services.

V. LIMITED LIABILITY OF THE PROVIDER

Art.10.

The PROVIDER shall not bear responsibility before the CLIENT and before third parties for the damages caused:

1. by the use of a qualified certificate issued on the ground of untrue/withheld information provided by the CLIENT;
2. by the use of the qualified certificate outside the limits of the restrictions for its effect;
3. by the fact that the CLIENT has not requested from the PROVIDER to terminate the effect of a qualified certificate, although he has found that the private key was unlawfully used or that there is a threat for its unlawful usage;
4. by failure of the provider to perform obligations as a result of technical problems beyond its control;
5. by failure of the CLIENT to fulfill his obligations envisaged herein or in the applicable policies and practices of the PROVIDER;
6. by use of unlicensed software by the CLIENT;
7. when signing with qualified electronic signature/seal: by use of a device which is not certified as a qualified electronic signature/seal device (QSCD) according to the Regulation;
8. by providing assistance to eliminate problems related to the installation and use of qualified certificates or services of the PROVIDER or of third parties, where the CLIENT has allowed access to the PROVIDER or third parties to work with his computer system or mobile devices.

VI. TERMINATION OF THE CONTRACT

Art. 11.

This contract shall be terminated:

1. upon expiry of the validity period of all qualified certificates issued under it;
2. upon termination of the qualified certificates issued under it;
3. upon occurrence of any other grounds specified in the applicable policies and practices of the PROVIDER.

VII. SUPPLEMENTARY PROVISIONS

Art. 12.

This contract may contain special terms and conditions that have priority with respect to the applicable policies and practices of the PROVIDER.

Art. 13.

The parties shall resolve any disputes arisen in the implementation hereof through negotiations between them and, failing this, they shall refer the dispute to the competent court in the city of Sofia, in accordance with art. 91 of the Civil Procedure Code.

Art. 14.

For any matters not regulated herein and matters related to the application of the PROVIDER's policies and practices, the provisions of the applicable legislation in the Republic of Bulgaria shall apply.

The applicable policies and practices of the PROVIDER, the Price Schedule for the service

provided, and the requests for providing certification services shall be an integral part hereof.

For the **PROVIDER**:

For the **CLIENT**:

DECLARATION – CONSENT BY THE SIGNATORY/CREATOR

№ ……

I, the undersigned:
……, PIN ……, permanent address: ……, telephone ……, e-mail address: ……..,
in my capacity as: natural person - SIGNATORY

DECLARE:

1. I am familiar with the requirements of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and certification services for electronic transactions in the internal market and repealing Directive 1999/93/EC (The Regulation), the related standards and the applicable law, as well as with the rules established in the policies and practices of the qualified provider of certification services "Evrotrust Technologies" Jsc., hereinafter referred to as PROVIDER.
2. I am familiar and agree with the applicable practices and policies, General Terms and Conditions of the contract for providing certification, information, cryptographic and consulting services, the Price Schedule for provided certification, information, cryptographic and consulting services, the Statement on the infrastructure of the public key (PKI Disclosure statement/PDS), and the remaining public documents published on the Evrotrust site related to the provided service.
3. I agree to perform all necessary actions for the issuance and management of certificates, according to the Provider's applicable policies and practices.
4. Upon violation of the integrity of the private keys used by me or of the access to them, I will inform the PROVIDER immediately.
5. I will store the private keys for the entire validity period of the certificates in a manner protecting them from compromising, loss, disclosure, modification and unauthorized use.
6. In the event that the PROVIDER provides me with a secure cryptographic device on which private keys are stored, I agree to use and change its access PIN code before using the certificates related to the private keys. The new PIN code shall be known only to me and I shall keep it secret.
7. I am informed that the PROVIDER uses and agree the PROVIDER to use records of the information used by me during registration, of the manner of provision of the device, including when it was provided to the SIGNATORY/CREATOR or to another party and each subsequent termination, identification attributes and other specific data included in the certificates, and the transfer of the information to third parties under the same terms and conditions as required under the applicable policy of the Provider, in the event that the latter terminates its services.
8. I agree the PROVIDER to collect, store and process my personal data and declare that I am informed that: the PROVIDER shall use them for the needs of its activity as a qualified provider of certification, information, cryptographic and consulting services; shall process and store them electronically and on paper; the provision of the personal data specified in the Regulation and the standards related to it and the applicable legislation is obligatory, the provision of any personal data outside of the framework of the activity of the PROVIDER under the Regulation and related standards and the applicable law is voluntary and the refusal to provide personal data

shall be ground for not concluding the contract or for its termination; recipients who can receive the data are the persons established by law; the access to the personal data for requesting changes shall be realized through the PROVIDER at the address provided on its Internet page http://www.Evrotrust.com.

9. I was informed that the provision of my personal data under the Law on Electronic Documents and Electronic Certification services (LEDETS) is mandatory. My refusal to provide my personal data required under LEDETS shall be ground for refusal to issue certificates.

For the **DECLARANT** (SIGNATORY/CREATOR):

REQUEST

to issue a qualified certificate for qualified electronic signature

Evrotrust Qualified Natural Person Certificate

Registration number: …… Registrar: ……

Data with Latin characters that shall be visible in the issued electronic certificate:

1. Signatory full name
2. Signatory unique identifier
Click or tap here to enter text.
3. E-mail to contact the Signatory Click or tap here to enter text.
4. Country code which determines the general context of the other attributes of the person

Information for additional identification/ verification:

Password:	.	.	.	.	.	.	.	.

The qualified provider of certification services, Evrotrust Technologies Jsc (PROVIDER), uses this password with a length of at least 4 characters to authenticate upon requests to suspend/ restore/ terminate a qualified certificate and during communication, with the purpose to identify the person.

I want the access to the certificate issued to me to be public ☐[i]

For the SIGNATORY:

[i] *By default, the Signatory has restricted access to his certificate*