GENERAL TERMS AND CONDITIONS FOR THE PROVISION OF QUALIFIED TRUST SERVICES

1. Preamble

1.1. This document represents the contract concluded between the Provider and the User, within the meaning of Article 1270 of the Romanian Civil Code, and establishes the conditions under which qualified trust services are to be provided.

1.2. The contract shall take full legal effect as of the date it is signed by the User or, as applicable, as of the date of its explicit acceptance by electronic means, without the need for an additional written instrument, as it contains all essential clauses concerning the parties, the subject matter, the term, the price, and the rights and obligations of the parties.

1.3. This contract is governed primarily by the following legal instruments: Law No. 287/2009 (Civil Code); Regulation (EU) No. 910/2014 (eIDAS) on electronic identification and trust services for electronic transactions; Law No. 214/2024 on the use of the electronic signature, the timestamp and the provision of trust services; Regulation (EU) 2016/679 (GDPR) on the protection of personal data.

2. Contracting Parties

ALFATRUST CERTIFICATION S.A., a legal entity incorporated under the laws of Romania, having its registered office in Romania, Bucharest Municipality, District 1, 155 Calea Victoriei, Building D1, Section 8, 9th Floor, EUID ROONRC.J40/8982/2004, Tax Identification Number (CUI) RO 16477015, bank account no. RO08BTRLRONCRT0528533501 opened with Banca Transilvania and account no. RO60TREZ7015069XXX012506 opened with the State Treasury, with the contact details indicated in the footer of this document, legally represented by Mr. Dragoș Soare, in his capacity as Administrator, hereinafter referred to as the "Provider"

and

Ms./Mr. [...], a citizen of [nationality], residing at [permanent or temporary address], identified by Identity Card/Passport Series [...] No. [...], issued by [...], valid from [...] until [...], holding Personal Numeric Code (CNP) [...], telephone number [...], e-mail address [...], in his/her capacity as the "User", hereinafter referred to as the "User".

3. Subject Matter of the Contract

3.1. The subject matter of this Contract is the provision of qualified trust services by the Provider, in accordance with the provisions of Regulation (EU) No. 910/2014 (eIDAS) on electronic identification and trust services for electronic transactions, Law No. 214/2024 on the use of the electronic signature, the qualified timestamp and the provision of trust services, and the Statement of Practices applicable to the trust services provided by AlfaTrust Certification S.A., as published on the Provider's official website and applicable to the contracted services.

3.2. Depending on the User's request, the services may include: the issuance of qualified digital certificates for electronic signature, electronic seal, qualified timestamp, or other trust services, in accordance with the applicable legislation.

3.3. The contracted services and the technical conditions are described in detail in the associated documents and policies published on the official website www.alfasign.ro, which form an integral part of this Contract.

4. Term of the Contract

4.1. This Contract shall enter into force on the date it is signed by the User or, as applicable, on the date of its explicit acceptance by electronic means (including by ticking the dedicated checkbox for the acceptance of the terms and conditions on the website). In the case of reissuance, the Contract may be signed by means of a valid qualified electronic signature certificate issued by a qualified trust service provider.

4.2. The term of this Contract shall be equivalent to the validity period of the qualified digital certificate issued pursuant hereto.

5. Price of the Contract

5.1. The price of the services provided under this Contract shall be determined according to the type of qualified trust service requested by the User, in accordance with the offer publicly displayed on the Provider's website or previously communicated by electronic means.

5.2. The exact value of the contracted service is indicated on the Provider's website or in the offer communicated to the User by the Provider and represents the consideration accepted by the parties under this Contract.

5.3. The tax invoice shall be issued in electronic format, based on the information provided by the User in the online form or in the order submitted, and shall be sent to the e-mail address provided by the User, in accordance with the applicable fiscal legislation.

6. Obligations of the Parties

6.1. Obligations of the Provider

6.1.1. The Provider undertakes to deliver the qualified trust services in strict compliance with the provisions of Law No. 214/2024, Regulation (EU) No. 910/2014 (eIDAS), Regulation (EU) 2016/679 (GDPR), other applicable regulations, and its Code of Practice and Procedures, available on the Provider's website.

6.1.2. The Provider undertakes to ensure complete and accessible information to the User, prior to the conclusion of the contract, regarding the terms of use of the services offered, including: the Provider's identity and contact details, the type of trust service requested and the corresponding certificate, the purposes and limits of use, the issuance, suspension and revocation procedures, potential risks, applicable fees, the rights and obligations of the parties, as well as its practice and security policies.

6.1.3. The Provider undertakes to perform the identification of the User by means compliant with the applicable legislation, prior to the issuance of the qualified certificate, either in person or by authorised and secure remote identification means.

6.1.4. The Provider undertakes to issue qualified digital certificates solely based on a complete and valid request from the User, after verifying the User's identity and complying with all legal and internal procedural requirements.

6.1.5. The Provider undertakes to record all qualified digital certificates issued under this Contract in its own electronic register, updated in real time. This register includes an internal database for operational records and a publicly accessible register available online on the Provider's official website, enabling any interested third party to verify, free of charge and on a permanent basis, the validity status of the certificates.

6.1.6. The Provider undertakes to implement appropriate organisational and technical measures to ensure the security of the IT systems used, the protection of personal data, the prevention of unauthorised access, loss or unauthorised alteration of data, and the availability and integrity of the service.

6.1.7. The Provider undertakes to suspend the qualified digital certificate within no more than 24 hours from becoming aware of a justified legal or contractual ground, including at the User's request, pursuant to a final court decision, or in other situations provided in the Code of Practice.

6.1.8. The Provider undertakes to revoke the qualified digital certificate within no more than 24 hours from the occurrence of any of the following situations: the User's request, the finding of inaccurate or false data, compromise of the signature creation data, the death or legal incapacity of the User, or pursuant to a final court decision.

6.1.9. The Provider undertakes to duly notify the User of the suspension or revocation of the certificate, indicating the reasons for the decision, its effective date, and the related legal consequences.

6.1.10. The Provider undertakes to promptly record in the electronic register the details regarding the suspension or revocation of a qualified digital certificate, in accordance with the applicable legislation. The issuance of a certificate is recorded automatically and in real time

at the moment of its generation. Revocation is performed manually and recorded in the public register within a maximum of 24 hours from the resolution of the revocation request.

6.1.11. The Provider undertakes to ensure free public access, in electronic format, to information regarding the validity status of qualified digital certificates (valid, suspended, revoked) through a system available in real time. Users and interested third parties may verify at any time the status of certificates, and the signing of documents with an expired, suspended or revoked certificate is technically impossible under the validation mechanisms implemented by the Provider.

6.1.12. The Provider undertakes to retain, for the period established by the applicable legislation, all documents and data related to the issuance, suspension, revocation, and expiration of certificates, in such a way as to allow the auditing of services and proof of compliance.

6.1.13. The Provider undertakes to promptly notify the competent authorities and take all necessary measures to remedy the situation in case of a security incident, major malfunction, or significant risks.

6.1.14. The Provider undertakes to process the User's personal data solely for the purpose of performing this Contract, in conditions of lawfulness, fairness, and transparency, in compliance with Regulation (EU) 2016/679 (GDPR), including the principles of data minimisation, storage limitation, and data security.

6.1.15. The Provider undertakes to cooperate with regulatory and supervisory authorities, to allow audits to be conducted, and to respond to their requests promptly and fully.

6.1.16. The Provider is obliged to perform the contracted services with professionalism, impartiality, confidentiality, and due diligence, at a quality level corresponding to the legal requirements and the legitimate expectations of the User.

6.2. Obligations of the User

6.2.1. The User undertakes to provide the Provider, in good faith, with accurate, complete, and up-to-date identification data, both at the time of requesting the services and throughout the validity period of the certificate.

6.2.2. The User undertakes to read and accept in advance the Terms and Conditions, the Privacy Policy, and the Statement of Practices applicable to the trust services provided by the Provider, all of which are publicly available, and to comply with them throughout the term of the contract.

6.2.3. The User is required to present the Provider with his/her identity document in physical format. In the case of physical identification, the person designated by the Provider shall: (1) make a hard copy of the identity document; (2) certify the copy with the statement "true to the original" affixed thereto; (3) indicate the current date on the copy; and (4) sign the copy by hand. In the case of remote identification, the procedure shall be carried out in accordance with the Provider's internal regulations on video identification and the recording of supporting documents.

6.2.4. The User undertakes to use the digital certificate solely for the declared purposes, within the limits and under the conditions set forth by the applicable legislation, by this Contract, and by the Provider's policies. Use for other purposes or beyond the declared limits may give rise to the User's contractual and/or legal liability.

6.2.5. The User undertakes to verify the accuracy of the data entered in the certificate upon receipt by using the certificate and to immediately notify the Provider of any discrepancy. In the absence of a notification within 5 (five) calendar days from the date of receipt of the certificate, it shall be deemed accepted. If the error is reported within the time limit, the certificate shall be revoked, and the Provider shall issue a new certificate with the correct data, in accordance with the applicable procedure.

6.2.6. The User undertakes to store, under maximum security conditions, the qualified device for creating the electronic signature and the signature creation data, not to disclose them to third parties, and to prevent any unauthorised or fraudulent use.

6.2.7. The User undertakes to notify the Provider without delay in the event of compromise, loss, theft, or unauthorised use of the signature creation data, in order to suspend or revoke the certificate.

6.2.8. The User undertakes to request the revocation or suspension of the qualified certificate if the essential data contained therein no longer corresponds to reality or in any other situation that may affect its validity.

6.2.9. The User undertakes to bear the cost of replacing the storage device (e.g., token) in the event that its damage, loss, or destruction is attributable to the User's own fault.

6.2.10. The User undertakes to refrain from any fraudulent use of the certificate and not to alter, forge, or transmit to third parties any incorrect data relating to his/her identity or the use of the qualified digital certificate.

6.2.11. The User is obliged to notify the Provider of any change in his/her contact details or of any situation that may affect the performance of this Contract.

6.2.12. The User undertakes to comply with the technical and procedural requirements established by the qualified trust service provider, in particular those set forth in the Code of Practice and Procedures and in the certification policies, made available through accessible means.

7. Acceptance of the Certificate

7.1. Upon receipt of the qualified digital certificate, the User is obliged to immediately verify its contents, with priority given to the following elements: the correctness and accuracy of the personal data entered in the certificate; the conformity of the certificate with the application and the documents previously submitted to the Provider. Any discrepancy or error identified must be notified to the Provider without delay, in accordance with Article 6.2.5 of this Contract.

7.2. Should any errors, discrepancies, or other irregularities be identified, the User is obliged to promptly notify the Provider, for the purpose of revoking or suspending the certificate, prior to any use thereof.

7.3. The certificate shall be deemed expressly accepted by the User if it is used for signing or authenticating any electronic transaction, or if no notification regarding errors or discrepancies is submitted within 5 (five) calendar days from the date of receipt of the certificate and the related cryptographic device, whether collected in person from the Provider's premises or delivered by courier.

7.4. Acceptance of the qualified certificate entails acknowledgment of its validity and the User's assumption of all legal effects arising from its use, in accordance with the applicable legislation.

8. Quality Standards Applicable to Qualified Trust Services

8.1. In providing qualified trust services, including the issuance of qualified digital certificates, the Provider shall comply with the relevant European and international standards regarding the security, interoperability, and quality of services, including but not limited to: ETSI EN 319 401 – General Policy Requirements for Trust Service Providers; ETSI EN 319 411-1 and ETSI EN 319 411-2 – Requirements for Certification Service Providers issuing Qualified Certificates; ETSI EN 319 411 parts 1 to 5; ETSI EN 319 421 – Policy Requirements for Trust Service Providers providing Long-Term Data Preservation Services; ETSI EN 319 422 – Policy Requirements for Time-Stamping Authorities issuing Qualified Timestamps; ISO/IEC 27001 – Information Security Management Systems; FIPS PUB 140-2 – Security Requirements for Cryptographic Modules.

8.2. The Provider undertakes to maintain compliance with the technical, organisational, and security requirements established under Law No. 214/2024, Regulation (EU) No. 910/2014 (eIDAS), and the audit and supervisory standards applicable to qualified trust service providers in Romania.

8.3. The Provider warrants that the devices and infrastructure used in the provision of services are tested, certified, and compliant with the security levels required by the applicable regulations, so as to ensure a high level of trust and data protection.

8.4. The Provider is subject to periodic audits performed by accredited independent bodies and to supervision by the competent authority, for the purpose of verifying compliance with the standards applicable to qualified trust services.

9. Processing of Personal Data

9.1. The Provider processes the User's personal data in accordance with the applicable data protection legislation, including Regulation (EU) 2016/679 (GDPR) and Law No. 214/2024. Details regarding the categories of data processed, the purposes, the legal grounds, the recipients, the storage period, the rights of the data subject, and the means of exercising such rights are available in the Privacy Policy published on the website www.alfasign.ro, which forms an integral part of this Contract.

10. Termination of the Contract

10.1. General cases of termination

This Contract shall terminate by operation of law, without notice, without prior notification, and without the intervention of a court of law or arbitral tribunal, in any of the following situations:

a) on the date of expiry of the qualified digital certificate issued under this Contract

b) on the date of revocation of the qualified digital certificate by the Provider, regardless of the reason for revocation, in accordance with the law and this Contract;

c) in the event of the User's express refusal to accept the qualified digital certificate

d) on the date on which the Provider loses its status as a qualified trust service provider, pursuant to the law;

e) on the date of termination, for any reason, of the framework contract concluded between the Provider and the legal entity on whose behalf the qualified digital certificate was issued, if and to the extent that the respective certificate is used for the electronic signature of that entity.

10.2. Termination by mutual agreement

The Contract may be terminated at any time by written agreement of the parties, without additional formalities.

10.3. Termination by unilateral rescission

The Contract may be terminated by unilateral rescission, pursuant to Article 1552 of the Civil Code (Law No. 287/2009), if one of the parties fails, quantitatively and/or qualitatively, to perform one or more of the essential obligations of this Contract. In such case, the aggrieved party shall notify in writing the defaulting party and, unless the latter is in default by operation of law, shall grant a remedy period of 5 (five) business days from the date of receipt of the notification. If the obligations are not duly and fully performed within this period, the aggrieved party shall have the right, but not the obligation, to notify the unilateral rescission of the Contract with effect from the date indicated in the rescission notice. Amounts already paid shall in no event be reimbursed, the principle of one-off performance of contractual obligations ("uno ictu") being applicable.

10.4. Termination by unilateral withdrawal

The User may unilaterally withdraw from the Contract, by written notice, in the event that he/she requests the revocation of the qualified digital certificate issued under this Contract.

10.5. Effects on the certificate

The termination of this Contract, regardless of the legal ground, shall result in the loss of the User's right to use the qualified digital certificate. The Provider shall proceed to revoke the certificate within no more than 24 (twenty-four) working hours from the moment it becomes unequivocally aware of the termination of the Contract, in accordance with the provisions of Law No. 214/2024 on the use of the electronic signature, the timestamp, and the provision of trust services based thereon.

10.6. Effects on due obligations

The termination of this Contract shall not affect the obligations already due between the parties at the date of termination, nor the rights and obligations relating to confidentiality, archiving, liability, and the protection of personal data, all of which shall continue to produce effects after the termination of the Contract.

11. Issuance and Reissuance of the Qualified Digital Certificate

All qualified digital certificates are issued as new certificates, whether it is the first issuance or a reissuance. Automatic extension of a previous certificate is not possible — each certificate has its own validity period and is installed either on a cryptographic device (token) or within secure cloud storage infrastructure, depending on the option chosen by the User.

11.1. Issuance of the Qualified Digital Certificate

11.1.1. The issuance of a qualified digital certificate represents the initial process by which a new certificate is generated, based on the completion of the registration form, the completion of the identification procedure, and the conclusion of a contract for the provision of qualified certification services.

The issuance of a qualified digital certificate takes place after the User completes the registration form available online on the Provider's website.

11.1.2. During the registration process, the User must:

- accept the Terms and Conditions of the trust service provider;
- accept the Personal Data Processing Policy (GDPR);
- provide all the information requested in the registration form.

11.1.3. After completing the form:

- if identification is carried out remotely (online), the User will receive by e-mail a secure link for video identification, in accordance with the procedure approved by the Competent Authority (ADR);
- if identification is carried out in person, the User shall sign the identification statement, sent by the Provider via e-mail, and present it duly signed at the Provider's headquarters or at the premises of authorised partners.

11.1.4. The qualified digital certificate shall be issued only after:

- successful completion of the identification process;
- payment of the service fee, according to the communicated invoice;

- signing of the contract for the provision of qualified certification services.

11.2. Reissuance (Renewal) of the Qualified Digital Certificate

11.2.1. The reissuance of a qualified digital certificate consists in the issuance of a new certificate with the same identification data, within an existing contractual relationship, for the purpose of replacing a previous certificate (e.g., in case of expiry, blocking, or loss). In case of reissuance, the same cryptographic device (token) is used, and the reissued certificate is installed by the User in place of the previous one. Reissuance does not require repeating the full issuance process, except where changes in identification data occur.

11.2.2. Reissuance means issuing a new qualified digital certificate, with the same data as the previous one, in the following situations:

- the existing certificate is about to expire;
- the certificate has been blocked as a result of a usage error;
- the contractual relationship with the Provider is to be continued, without any change in the identification data.

11.2.3. Reissuance is permitted only if:

- the previous certificate has not expired;
- the certificate has not been revoked;
- the identification data contained in the previous certificate have not changed.

11.2.4. The User is obliged to request the reissuance of the certificate at least 3 business days prior to the expiry date, in order to ensure continuity of the contractual relationship and the services provided.

11.2.5. In the case of reissuance:

- the Provider shall send the User, at the e-mail address specified in the valid certificate, a prior notice regarding the impending expiry, at least 5 days before the expiry date;

- the Provider shall request confirmation that the identification data have not changed. If they have changed, the User shall complete a new online form and follow the full issuance process (Article X.1);

- if the data are identical, the Provider shall issue a proforma invoice and send the video identification link, in the same manner as in the initial procedure.

11.2.6. After successful completion of the identification process and confirmation of payment, the Provider shall issue the new qualified digital certificate, which shall be:

- delivered to the User via e-mail, in an archived format;

- installed by the User on the same previous token (the old certificate being overwritten).

Reissuance shall be performed at no additional cost in case of blocking of the cryptographic device (token), and the new certificate shall have the remaining validity period of the previous certificate.

All certificates issued, including those obtained through reissuance, are new certificates, digitally signed and recorded in the Provider's internal systems.

12. Contractual Liability

12.1. The Parties shall be liable for non-performance, delayed performance, or improper performance of the obligations assumed under this Contract, in accordance with Articles 1350 et seq. of the Civil Code and the applicable special legal provisions.

12.2. The qualified digital certificate issued is strictly personal and may be used only by the designated person (the User) identified in its content. It has the same legal value as a handwritten signature. The transfer of the cryptographic device or the related data (private key, codes) to other persons, their use by such persons, or the delegation of access is strictly prohibited. The Provider is released from liability for any damages or legal consequences arising from unauthorised use of the certificate in breach of the foregoing.

12.3. The User undertakes to comply with all security measures, technical and legal instructions communicated by the Provider through the Code of Practice and Procedures, the

usage policies, and this Contract. Failure to comply with these shall release the Provider from any liability.

12.4. The Provider shall not be liable for damages caused by: use of the certificate after its expiry, suspension, or revocation; use of the certificate by a person other than the designated User, regardless of purpose; loss, disclosure, or compromise by the User of the cryptographic device or authentication data (PIN, activation codes); use of the certificate for purposes contrary to those declared, to the law, or to the instructions set out in the Code of Practice and Procedures; provision of incorrect data by the User in the certificate application; installation or use of unauthorised applications/devices that affect the functioning of the certificate; force majeure or fortuitous events preventing the Provider from fulfilling its obligations.

12.5. The Provider shall not be liable for indirect damages, including but not limited to loss of profit, loss of revenue, loss of business opportunities, or business interruption; the economic consequences arising from the use, inability to use, or malfunction of the certificate; or third-party claims exceeding the lawful scope of certificate use.

12.6. Any damages awarded by the Provider shall be limited to the actual proven loss and shall in no event exceed the value of the service paid by the User for the respective qualified digital certificate.

12.7. The Provider shall not be liable for delays, suspensions, or revocations caused by the requirements or actions of regulatory or supervisory authorities.

12.8. Neither party shall be liable for failure to perform contractual obligations where such failure is caused by a force majeure event, as defined by law. The affected party shall notify the other party within 5 business days from the occurrence of the event.

13. Legal Guarantee of Conformity

The products and services delivered to consumers benefit from the legal guarantee of conformity provided by the applicable legislation (Government Emergency Ordinance No. 140/2021 on certain aspects concerning contracts for the sale of goods, and Government Emergency Ordinance No. 141/2021 on certain aspects concerning contracts for the supply of digital content and digital services, as applicable).

14. Applicable Law and Dispute Resolution

14.1. This Contract shall be governed by Romanian law.

14.2. The Parties shall make every effort to resolve amicably any disputes arising in connection with the conclusion, performance, or termination of this Contract.

14.3. If an amicable settlement is not possible, the disputes shall be resolved by the competent courts of law, in accordance with the applicable legal provisions.

15. Miscellaneous Provisions

15.1. All communications, notifications, requests, or any other information necessary for the performance of this Contract shall be made in writing, by any of the following means: in person, with acknowledgment of receipt; by post/courier services with acknowledgment of receipt; through a court bailiff; by electronic means, signed with a valid qualified digital certificate.

If the same communication is sent by multiple means (e.g., post and qualified e-mail), the valid date shall be considered the one closest to the moment of confirmed receipt.

15.2. This Contract may be amended only by written agreement of both Parties, expressed through an addendum signed either in handwritten form or with a valid qualified digital certificate.

If this Contract and its annexes are signed by the User by qualified electronic means, the Provider shall send the signed copy of the Contract, together with the electronically signed tax invoice, to the e-mail address communicated by the User in the registration form or subsequently, during the contractual relationship.

USER: PROVIDER,

_____ ALFATRUST CERTIFICATION S.A.