

**GENERAL TERMS and CONDITIONS for
Qualified Electronic Signature and
Qualified Electronic Time Stamp Service**

Concluded today _____ between:

DIGISIGN S.A. joint-stock company with headquarters in Str. Virgil Madgearu 2 – 6, sector 1, Bucharest, phone: +40316202000, fax: +40316202080, e-mail: office@digisign.ro, registered at the Trade Register under no. J40/8069/2005, VAT registration no. RO17544945 and IBAN Code RO54 BTRL 0480 1202 W366 21XX opened at Banca Transilvania – Chibrit Branch, as Qualified Trust Service Provider granted by Romanian Supervisory Body – as per MCSI Order no. 833/22.08.2017, duly represented by Mr. Catalin Cuturela as General Manager, hereinafter referred to as DigiSign, and

USER, the natural persons identified as follows: _____ residing in _____, born on _____, identified by ID, series _____ number _____, issued by _____, valid between _____ and _____ having the unique personal identification number _____, e-mail _____ and phone _____.

1. Definitions

Qualified trust service means all and any of the qualified trust services provided by DigiSign as a Qualified Trust Service Provider, regarding the issuance, administration, suspension, revocation, renewal and validation of qualified digital certificates, according to EU Regulation no. 910/2014, the EC decisions laying down its application and the relevant national legislation in force, as well as all other additional services referred at www.digisign.ro, including, but not limited to, any electronic service usually provided in exchange of a fee, which consists of creation and validation of electronic signatures, electronic seals, electronic time-stamps and the certificates related to those services.

User means the natural person in whose name the qualified certificate is issued and which creates an electronic signature. The User can be the natural person which acts on his/hers behalf or a natural person acting as a designated representative of a legal person.

Beneficiary means a natural person or a legal person who orders and bears the cost of the trust service provided by DigiSign. The Beneficiary can be the same as the User or can be a different entity.

Qualified certificate for electronic signature means a certificate for electronic signatures that is issued by a qualified trust service provider and meets the requirements laid down in Annex 1 of EU Regulation no. 910/2014.

Qualified electronic signature creation device means an electronic signature creation device that meets the requirements laid down in Annex II of EU Regulation no. 910/2014.

Qualified electronic signature means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures issued by a Qualified Trust Service Provider.

Electronic time stamp means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.

Qualified electronic time stamp means an electronic time stamp that meets the following requirements:

- it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;
- it is based on an accurate time source linked to Coordinated Universal Time; and
- it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.

Electronic document means any content stored in electronic form, in particular text or sound, visual or audiovisual recording.

Code of Procedures and Practices hereinafter referred to as CPP, means both the Code of Practices and Procedures DigiSign and the Code of Practices and Procedures of DigiSign Time-Stamping Authority, being publicly available at www.digisign.ro.

DigiSign Certification Policy hereinafter referred to as CP, means the Certification Policy of DigiSign Certification Authority, being publicly available at www.digisign.ro

PKI Disclosure Statement, hereinafter referred to as PDS, means a public statement intended to be a supplementary and simplified tool that for Users and Beneficiaries, regarding the proper use of the trust services provided by DigiSign.

Personal data means any information about an identified or identifiable natural person („the Person”); an identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or many specific elements of his physical, genetic, psychic, economic, cultural or social identity.

All other definitions included in the EU Regulation no. 910/2014 on electronic identification and trust services for electronic transactions in the internal market shall apply, as well as the definitions in the applicable legislation and the definitions stated in CPP and CP.

2. Object

- This document states the general terms and conditions regarding the qualified trust services provided by DigiSign and ordered by the Beneficiary and/or User.
- DigiSign provides the qualified trust services in accordance with the applicable CPP and CP, this documents being considered a part of these terms and conditions.
- By submitting a request of qualified trust services to DigiSign represents acceptance of these terms and conditions. DigiSign shall not provide the qualified trust service requested if the User does not comply with the procedures regarding identification, in accordance with national applicable legislation, and/or if the User does not accept these terms and conditions.

3. Validity

This document shall enter into force at the moment it is signed by the Beneficiary of the Qualified Trust Service Agreement and it is valid for the entire period of the qualified certificate, not exceeding 3 years.

4. Services

In order to provide the qualified trust services requested, DigiSign ensures the following:

4.1. Certificate issuance

- 4.1.1. The issuance of a qualified certificate is made in accordance with the provisions of the applicable CP and CPP, as well as with the instructions published at www.digisign.ro.
- 4.1.2. At every issuance of a qualified certificate for electronic signatures, DigiSign verifies, with support of the registration authorities and in compliance with the national legislation, the identity and, if the case, the specific attributes of the natural person assigned as future title-holder of the digital qualified certificate.
- 4.1.3. The possibility to opt for the use of a pseudonym is assigned to applicants provided that it does not refer to expressions that are established to be inappropriate or that involve fraudulent usurpation of a known name, or parody of a person.

4.2. Certificate renewal

- 4.2.1. Before the end of the validity period of a qualified certificate, DigiSign undertakes to notify the User in this regard with 45, 30, 15, 7 and 2 days before the expiration date.

4.2.2. The certificate renewal is available for those Users which are in possession of a qualified certificate and request the continuity of it. The renewal procedure is made in accordance with the applicable CP and CPP, as well as with the instructions published at www.digisign.ro.

4.2.3. The certificate renewal is available also through electronic means, only to those Users in possession of a valid qualified certificate issued by DigiSign and provided the Users make a request of renewal with at least 5 (five) days prior to the expiration of the certificate.

4.2.4. The identification of the User, which makes a request of renewal, shall be made using the same procedures as for the issuance of a digital qualified certificate.

4.3. Digital Certificate revocation

4.3.1. Revocation of a digital certificate means the cancelation of its validity, the action being definitive, without the possibility to return to the certificate's initial status.

4.3.2. The revocation of a certificate is made in accordance with the provisions of the applicable CP and CPP, as well as with the instructions published at www.digisign.ro.

4.3.3. DigiSign shall promptly inform the User about the certificate revocation, together with the reasons for its decision.

4.3.4. DigiSign shall enclose the certificate revocation in the electronic register, within 24 hours of becoming aware of the respective decision, the revocation becoming thus enforceable against third parties from the date of its enrollment in the electronic register. Also, DigiSign shall insert the revoked certificate into the Certificate Revocation List.

4.3.5. DigiSign shall provide to any interested party information about the status of a certificate (e.g. active, revoked, suspended, and expired). This information shall be made available for each certificate issued, at any given time, including after the expiration of the certificate, in an automatic, reliable, free of charge and efficient way.

4.3.6. Revocation of a qualified certificate shall be made within 24 hours from the moment when DigiSign acknowledges the occurrence of any of the following:

(a) at the request of the User and/or Beneficiary, after a preliminary verification of his/hers identity, and in accordance with the instructions published at www.digisign.ro.

(b) in case the User of the certificate dies or a definitive court order is issued;

(c) in case it is undoubtedly proven that the certificate was issued on the basis of incorrect or false information or the essential data on the basis of which the certificate was issued are no longer true to reality.

(d) in case it is proven that the qualified certificate is fraudulently used or if the signature creation data have been compromised.

(e) upon the expiration of the maximum period for which the certificate may be suspended.

(f) in any of the cases provided under item 4.8.2. of CPP.

4.4. Suspension of a Digital Certificate

4.4.1. Suspension of a qualified certificate means the temporary revocation of a certificate, being made in accordance with the provisions of the applicable CP and CPP, as well as with the instructions published at www.digisign.ro. The maximum period of time on which a certificate can be suspended is 30 (thirty) days.

4.4.2. DigiSign shall promptly inform the User and/or Beneficiary about the certificate suspension, together with the reasons for its decision.

4.4.3. Suspension of a qualified certificate shall be made within 24 hours from the moment when DigiSign acknowledges occurrence of any of the following:

(a) at the request of the User and/or Beneficiary, after a preliminary verification of his/hers identity, and in accordance with the instructions published at www.digisign.ro.

(b) in case the suspension is requested by a final court order.

(c) on the occurrence of any of the events described at art. 4.3.6., under the conditions there is only a suspicion of the same.

(d) in any other situation where additional information from the User and/or Beneficiary is needed.

4.5. Digital Certificate Verification and Validation

4.5.1. Upon the certificate's acceptance by the User, DigiSign publishes in the electronic register of evidence, the public key of the certificate, thus the certificate becoming enforceable against third parties. Thereby, any interested party can verify the certificate by consulting the electronic register of evidence at www.digisign.ro.

4.5.2. In case of revocation or suspension, the certificate shall be inserted in the Certificate Revocation List published every 24 hours and shall remain valid for 48 hours.

4.5.3. to any interested party in verification of a certificate issued by the DigiSign Certification Authority, its validation in real time through the OCSP protocol.

5. DigiSign Obligations and Liabilities

5.1. DigiSign undertakes the obligation to comply with the provision of the applicable CP and CPP, as well as the provision of European and national applicable legislation. Thus, the main obligations of DigiSign are:

(a) to comply with the general terms and conditions states in this document, as well as with all applicable policies and practices published at www.digisign.ro

(b) to not issue a certificate without the preliminary verification of the User's identity, in accordance with the applicable national legislation, or without the validation of the documents on the basis of which the certificate is being issued.

(c) to ensure the security of the information systems used for providing certification services, using the practices unanimously recognized in the field and recommended by international standards.

(d) to issue the requested certificate within 5 working days from the receipt of the correct and complete documentation required for the certificate issuance process, unless the User and/or Beneficiary expressly requests another date beyond those 5 days.

(e) to publish in the electronic register of evidence the qualified certificates accepted by their Users.

(f) to publish the Certificate Revocation List in accordance with the provision of the applicable CP and CPP.

(g) to notify the User regarding (1) the rejection of the request to issue the certificate and the reasons regarding this decision, as well as the possible remedies, if any, (2) the issuance of the requested digital certificate, as well as the instructions regarding the proper use of the certificate, (3) the expiration period of the certificate and (4) regarding revocation/suspension of the certificate.

(h) to process revocation and suspension requests within 24 hours from the receipt and to verify the applicant's identity.

(i) to process personal data in a proper way, in accordance with the applicable legislation in force.

5.2. In the event of non-compliance with the obligations stated in the applicable legislation regarding the provision of qualified trust services, DigiSign shall be liable for the damages caused to any natural or legal person. DigiSign is liable for the damages caused intentionally or negligently

to any natural or legal person that bases his/hers/its conduct on the legal effects of the qualified certificates, but only in respect of:

- (a) the accuracy of the information contained in the certificate, at the issuing moment;
- (b) at the issuing moment, the dissemination to the User of the creation and validation data of signatures and time stamps
- (c) the immediate and permanent interruption of access at the creation and validation data of signatures and time stamps, under the condition that DigiSign has been duly notified
- (d) all other cases stated in the applicable legislation in force, at the issuing moment.

6. User obligations and liabilities

6.1. By signing these terms and conditions, the User declares that he/she acknowledged and undertakes the following obligations:

- (a) to provide all information required by DigiSign, complete and correct, for the purpose of registration and issuance of a qualified certificate
- (b) to consent that DigiSign shall process and store his/her personal data, as well as to retain a copy of the identification card, in order to perform necessary operations regarding the provision of the qualified trust services required, including the use of some of these data to create, maintain and publish the electronic register of evidence, in accordance with the applicable legislation in force.
- (c) to use only those secure cryptographic devices and software applications recommended by DigiSign, if the User generates the cryptographic key pair on its own; in this case, the User must express his option in writing, the request being attached to the present document and, as well, to provide DigiSign with a declaration as he/she complies with the standards for generating cryptographic key pairs used and recommended by DigiSign.
- (d) to use the qualified certificate only for its declared purposes and complying with its applicable scope, in accordance with the provision of the CP and CPP of DigiSign Authorities;
- (e) to comply with the guides and instructions issued by DigiSign regarding the proper use of the qualified certificates and the cryptographic devices, and not to exceed the limits stated in these terms and conditions
- (f) to request DigiSign to immediately revoke or suspend the certificate, in the event of the causes specified under art. 4.3 and 4.4.
- (g) to comply with these general terms and conditions, as well as with the applicable policies and procedures issued by DigiSign in force, available on www.digisign.ro;
- (h) to verify the content of the qualified certificate at the time of its receipt, in particular the correctness of data and the complementarity of the public key with the private key held, and in the case of a nonconformity, to request the revocation of the certificate immediately. If the User does not notify DigiSign of any irregularity in 5 days from acknowledgement, the certificate is deemed to be accepted by the User. Likewise, the certificate is considered accepted by the User from the moment he/she makes the first cryptographic operation with it. Each qualified certificate accepted by its User, is published in the electronic register of evidence of certificates issued by the DigiSign Certification Authorities, available on www.digisign.ro.
- (i) to notify DigiSign immediately of any change in his/hers identification data
- (j) not to attempt, in any way and by any means, to access or to modify DigiSign's database or equipments
- (k) to use the qualified trust services in good faith and not to engage DigiSign's liability in any way if the qualified trust services have been used in bad faith or in an unauthorized way.

6.2. Any non compliance of the User with its obligations shall be considered a breach of these terms and conditions and shall entail the revocation of the certificate and DigiSign's rights to claim damages.

7. Limitations, restrictions and exclusions

- 7.1. Qualified digital certificates for electronic signatures can be used only for cryptographic operations such as authentication, creation and validation of electronic signatures and time stamps and only by their User. It is prohibited to use the qualified certificate for electronic signature in other scope than those indicated and allowed by DigiSign and it is prohibited to use an expired, suspended or revoked certificate in order to create electronic signatures and/or time stamps.
- 7.2. The qualified trust services provided by DigiSign shall be used only in compliance with the instructions and guides issued by DigiSign, and in case of a breach of those, DigiSign shall be relieved of liability of any damages resulting from the use of the services that exceeded those instructions and guides.
- 7.3. DigiSign is not liable for (a) the damages caused by force majeure and/or unforeseeable circumstances (acts of God), (b) the damages caused by the inappropriate use of the qualified trust services, (c) the damages caused by the storage of erroneous data in DigiSign's database and their inclusion in the certificates issued for the User, in case the User declared that those data are correct, (d) the damages caused by the theft or the deterioration of the devices used to store the certificates, the unauthorized or improper use of them or any negligence of the User regarding their storage and use.
- 7.4. DigiSign does not take liability for and cannot be forced to pay damages for indirect prejudices, potential benefits or profits, financial loss, customer loss of data loss. In case of such a claim to cover prejudice, DigiSign liability is limited to the cost of the service delivered/for each claim of such type.
- 7.5. DigiSign reserves the right to refuse to issue a qualified certificate to those applicants who do not have the full capacity to exercise their rights under the applicable national legislation or if they lack the ability to read and/or write.

8. Confidentiality. Processing of personal information

- 8.1. DigiSign collects, processes, stores and archives personal data for the purposes of providing the qualified trust services required and only in compliance with the applicable legislation in force, under conditions that insure confidentiality of all information entrusted on it upon execution of the contract and during its implementation.
- 8.2. The User must provide his/her personal data so that DigiSign is able to deliver the qualified trust services requested and the refusal of the User to provide such data entails the impossibility of providing those services.
- 8.3. In compliance with Law no. 455/2001 regarding the electronic signature, as a Qualified Trust Service Provider, DigiSign has the obligation to keep the data on the basis of which the qualified certificate has been issued for a period of 10 (ten) years after the expiration date of that certificate. Beyond this term, personal information and data concerning the certificate shall be deleted in accordance with the applicable legislation on archiving. Thus, the User may exercise his/hers right to be forgotten, provided the mandatory period of data protection has lapsed.
- 8.4. DigiSign and its agents shall ensure the confidentiality of personal data provided by or requested from the User, unless the disclosure of such data is made with the prior consent of the User given under the present terms and conditions, or the disclosure of such data is made by authorized third parties or for rendering services by third parties (such as printing, dispatching invoices, debt collection services etc). Similarly, it shall be possible to disclose personal information to auditors, third parties the conduct of which depend on the certification services provided by DigiSign, also to monitoring or certification bodies, as well as to public institutions or bodies, affiliates of DigiSign and in any other situations duly justified upon prior notice of the User, as to serve the previously-mentioned purposes while protecting the User's rights.
- 8.5. DigiSign reserves the right to process personal data for promotional purposes, complying with the User's rights according to the applicable legislation in force. If these operations are performed by third parties, personal data may be communicated to them. The User shall be able at any time to withdraw his/hers consent regarding the use of personal data for promotional purposes, by written request, which upon being notified to DigiSign, it becomes part of these terms and conditions. Thus, regarding the processing of personal data for promotional purposes, the User has: (a) the right to information, (b) the right of access to data, (c) the right to interfere with data, (d) the right to object and (e) the right not to be the subject of an individual decision, and (f) the right to file complaints to the National Supervisory Authority for Personal Data Processing (dataprotection.ro), as supervisory authority.
- 8.6. The User undertakes the obligation to keep the confidentiality, in compliance with the Privacy Policy in force at the issuing date, published at www.digisign.ro.

8.7. Both DigiSign and the User shall be relieved of liability of disclosing confidential information if: (a) the information was known to a Party before it was communicated by the other Party, (b) the information was disclosed after the written consent of the owner of that information was obtained, or (c) the Party who was required to keep the confidentiality was legally obliged to disclose that information.

8.8. The disclosure of any confidential information to persons involved in the process of providing qualified trust services shall be confidential and shall comply with the provision of Regulation no. 679/2016 and shall only extend to the information necessary to carry out the activities of those persons.

8.9. A third party may have access only to the information publicly available in certificates (i.e. name, surname, email). The other information provided in the applications delivered to DigiSign shall not be disclosed under any circumstances to a third party, intentionally or not (except for the situations where the law requires such disclosure).

8.10. The present confidentiality terms shall be complemented by the national and European legislation on personal data processing.

8.11. The information notice on personal data protection is available on https://www.digisign.ro/uploads/Protectie_date.pdf.

9. Termination

These terms and conditions shall cease in any of the following situations:

(a) upon expiration or revocation of the qualified digital certificate;

(b) upon rejection of certificate application;

(c) upon failure to accept the certificate by the User;

(d) within 30 (thirty) days of receipt of a notice sent by DigiSign regarding the breach of the obligations assumed by the User under the general terms and conditions, provided this violation has not been remedied within this interval.

(e) in case of termination of the qualified trust service contract between DigiSign and the Beneficiary.

If these terms and conditions cease, the revocation of the qualified certificate is being entailed, in the case the certificate remains active. Termination of the Contract has no effect on the pending obligations between the parties.

10. Availability

10.1. DigiSign ensures working days from Monday to Friday between 9 AM and 5 PM, with the exception of Romanian legal holidays and runs for the benefit of the Users and any interested parties a HelpDesk department available 24/7 at the number 031 620 12 89 or by e-mail at helpdesk@digisign.ro regarding any information about the qualified trust services provided by DigiSign, as well as for any relevant additional services.

10.2. DigiSign guarantees to the persons with disabilities access to its headquarters on Str. Virgil Madgearu 2 – 6, sector 1, Bucharest, Romania by means of a special arranged parking space, an access ramp and a lift with sound and visual indications.

11. Settlement of Litigation

11.1. All disputes or conflicts arising from the Contract or its execution shall be amicably settled by representatives of the Parties, as per the civil law.

11.2. In case the amicable settlement of disputes or conflicts fails, the cause shall be referred for settlement to the competent court of justice at DigiSign headquarters as per the applicable Romanian legislation in force.

12. Notifications

12.1. Any notifications between Parties shall produce legal effects only if made in writing, as follows: by e-mail, by registered mail or by facsimile with delivery confirmation report.

12.2. DigiSign shall deliver in person to the User the qualified digital certificate stored on the secure cryptographic device, together with the related documents, as per the User's option expressed on the form application submitted to DigiSign:

At DigiSign's headquarters or at the location where the representative of DigiSign performed identification of the User

These general terms and conditions were drawn up in two copies, one for each Party, both having the same legal value.

Provider,

USER

DigiSign SA

Through its representative,