LISBOA
Lagoas Park, Edifício 3, Piso 3
2740-266 Porto Salvo
Oeiras – Portugal
Tel.: +351 217 123 010
Fax: +351 217 123 011

PORTO
Av. Sidónio Pais, 379
Ed. Hoechst A, Piso 3, Dto.
4100-468 Porto – Portugal
Tel.: +351 223 391 810
Fax: +351 223 391 811

GENERAL TERMS AND CONDITIONS OF DIGITAL CERTIFICATE ISSUANCE

SECTION 1 – DEFINITIONS

For the purposes of this 'General Terms and Conditions' and unless otherwise expressly resulting from its text, the following words and expressions shall have the meaning stated as follows:

1.1 MULTICERT: Certifying Authority, named MULTICERT – Serviços de Certificação Electrónica, S.A, a corporation with registered office at Lagoas Park, Building 3, 3rd Floor, Porto Salvo – Oeiras, and capital stock of € 2.250.000, legal person number 505 767 457, registered before the Commercial Registry Office of Amadora (1st CRPC Amadora).

1.2 Certification Authority: entity which creates or provides means to the creation and verification of the Digital Certificates (DCs), issues and manages the lifecycle of the DCs, ensures their publication and provides other services related with digital certificates.

1.3 Trust Service Provider: natural or a legal/collective person who provides one or more trust services either as a qualified or as a non-qualified trust service provider (Regulation (EU) No 910/2014 of the Parliament and of the Council of 23 July 2014).

1.4 Qualified Trust Services Provider: trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body (Regulation (EU) No 910/2014 of the Parliament and of the Council of 23 July 2014).

1.5 Certificate holder: natural or legal person identified in a Digital Certificate (DC) as the holder of the DC issued by MULTICERT, who is responsible by its use and who is obliged to comply with the conditions for use of the digital certificate and other conditions established in this document.

1.6 "Legal Representative" of a legal/collective person certificate holder: person responsible for the use of a Digital Certificate issued for Collective Person Representation Purposes. The legal representative is obliged to the same conditions as the CLIENT and is, in this document, identified as such.

1.7 Client: person who requests the issuance of a DC and concludes the corresponding contract; the issuance of a DC can be required by the certificate holder himself or by a third party who requires it on behalf of the certificate holder.

1.8 Client`s Responsible person: person empowered to bind the CLIENT, when this is a legal/collective person, powers which are verified through official document.

1.9 Supervisory Body: an entity designated by each Member State to: i) supervise qualified trust service providers established on the territory of the designated Member State to ensure, by means of a priori supervisory activities and a posteriori, that the providers and qualified trust services provided by them fulfill the requirements laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council; ii) if necessary, take action against unqualified trust service providers established on the territory of the designating Member State through ex post supervisory activities if it is alleged that such service providers or trust services provided by them do not comply with the requirements laid down in Regulation (EU) No 910/2014 of the

European Parliament and of the Council. In Portugal, the Supervisory Body is constituted by the Nacional Security Authority.

1.10 Registration Authority: entity that provides to MULTICERT the services related to the certificate holder and the CLIENT's identification, the conclusion of digital certificate issuance and management, services which are not assigned exclusively to MULTICERT as Certification Authority.

1.11 Digital Certificate (DC): electronic document which connects the data for verifying the digital signature of its certificate holder and confirms the certificate holder's identity. The DC is issued by MULTICERT according to X.509v3 standard, defined by the ITU (*International Telecommunication Union*). In this document, a DC refers to an Advanced Digital Certificate or a Qualified Digital Certificate.

1.12 Advanced Digital Certificate (ADC): certificate which allows ensuring the authenticity and integrity of the electronic documents to which the signature of the certificate holder has been added, as well as checking if the electronic document was changed after that signature had been added. The ADC is issued by MULTICERT according to MULTICERT's CPS (Certification Practices Statement).

1.13 Certificado Digital Qualificado (CDQ): certificado que contém indicação de que o certificado é emitido como certificado qualificado, pode conter um atributo específico do titular, restrições ao âmbito de utilização e é emitido por entidade certificadora que reúne os requisitos definidos no Regulamento (UE) nº 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014. O CDQ é emitido pela MULTICERT conforme a DPC (Declaração de Práticas de Certificação) da MULTICERT.

1.14 Qualified Digital Certificate (QDC): certificate which holds indication that the certificate is issued as a qualified certificate, may contain a specific attribute of the certificate holder, restrictions on the scope of use and is issued by a certification authority complying with the requirements defined in the Regulation (EU) No 910/2014 of the Parliament and of the Council of 23 July 2014. The QDC is issued by MULTICERT in according to MULTICERT`s CPS (Certification Practice Statement).

1.15 PKI MULTICERT (Public Key Infrastructure MULTICERT): set of services provided by MULTICERT, as Certification Authority, or by the Registration Authority, as established in the Digital Certificate Issuance Agreement, concerning the DCs' issuance, based on the public key technology, applications, policies, practices and standards adopted by MULTICERT, and corresponding management, in order to ensure security and trust in electronic communications.

1.16 Certification Practice Statement (CPS): document in which are described the certification practices used by the certification authority during the certificate management process, available at https://pki.multicert.com/.

1.17 Certificate Policy (CP): set of rules which define the applicability of a DC in the context of a certain community of clients, available at https://pki.multicert.com/.

1.18 Electronic document: document elaborated through data electronic processing.

1.19 Private Key: element of the asymmetric key pair meant to be known only by the certificate holder, through which an electronic document can be signed, ensuring the authenticity of the sender and that the information exchanged was not modified in its path from the sender to the recipient.

1.20 Public Key: element of the asymmetric key pair meant to be disclosed, with which the digital signature added on the electronic document by the certificate holder of the asymmetric key pair is verified, wherein if the signature is valid, we may conclude that the message was not modified in the path from the sender to the recipient, and that it was the sender who indeed sent the message.

1.21 DC Reissuance / Reissued DC: DC issued when the maximum period of validity of a digital certificate is reached, as provided in Section **6**. The Reissued DC will be subject to other provisions of this General Terms and Conditions.

1.22 Remote Signature Generation Service Provider: based on the trust services of electronic signature and electronic seal, that allows the remote management of the device for certificate holder`s signature generation and the generation of electronic signatures by mean of a device remotely managed, in accordance with the Order 155/2017 of the National Security Authority and the Regulation (EU) No 910/2014 of the Parliament and of the Council.

1.23 Remote Signatures in Cloud or Token Cloud: remote service available by MULTICERT for the custody and usage of certificate key. See definition of Remote Signature Generation Service Provider.

1.24 Force Majeure event: any unexpected and insuperable event, beyond the will or control of the party and which prevents it, totally or partially, permanently or temporarily, to meet its obligations. Can be considered Force Majeure events, namely, a state of war, declared or not, rebellion or riot, natural disasters, as fires, floods, earthquakes, extended power and/or communication failures and prolonged transport strike.

SECÇÃO 2 – GENERALIDADES

2.1. By concluding a Digital Certificate Issuance Agreement, MULTICERT agrees to provide to the CLIENT the Digital Certificate (DC) issuance services as well as other services related to the certification activity and the CLIENT agrees to use the DC in the terms and conditions established in this document.

2.2. The Digital Certificate Issuance Agreement is considered to be concluded on the date in which the Agreement Form is accepted by MULTICERT (or by MULTICERT's Registration Authority), which will occur after the CLIENT's subscription of the Agreement Form for concluding that agreement and presented, or delivered of the required documentation.

2.3. The issuance of the DC and further contractual relationship between MULTICERT and the CLIENT are ruled by this 'General Terms and Conditions' and by the legal provisions and regulations concerning the issuance of digital certificates and the activity of the certification authority (Regulation (EU) No 910/2014 of the Parliament and of the Council).

2.4. In light of the technological progress which the area of electronic certification may suffer, MULTICERT will perform the steps reasonably required to improve the service which is object of this Digital Certificate Issuance Agreement and the compliance with new technical and regulatory standards. MULTICERT may make amendments and procedural or technical adjustments deemed necessary for the efficient execution of the Digital Certificate Issuance Agreement. Contractual amendments arising therefrom shall meet the rules in Section 12.

2.5. MULTICERT does not ensure the continuous operation of the computer system which supports the services which are object of the Digital Certificate Issuance Agreement, namely if the computer system suffers technical correction interventions, required for compliance of MULTICERT's PKI with any legal or regulatory changes, or in order to improve or enhance the aforementioned computer system.

2.6. The obligations undertaken by MULTICERT are limited to the provision of means, thus not ensuring to the CLIENT or the certificate holder the achievement of their specific intended outcomes.

2.7. MULTICERT ensures that the creation and issuance of the digital certificate and the key pairs, as well as all components of MULTICERT's PKI comply with the applicable technical safety standards in the current state of the art.

2.8. MULTICERT CA is a certification authority accredited by the National Security Authority (http://www.gns.gov.pt/gns/pt/tsl/), as provided by European and Portuguese laws, and is therefore legally capable of issuing all types of digital certificates, including qualified digital certificates (digital certificates with the highest degree of security/trust provided by law).

SECTION 3 – MULTICERT`S OBLIGATIONS

A MULTICERT is obliged to:

3.1. In case it accepts the Agreement Form, issue or renew the DC, proceeding to the new key pair generation according to legal provisions, regulatory requirements or regulations issued by the European Parliament and/or Supervisory Body.

3.1.1. Issue the DC based on the data and information provided by the CLIENT.

3.1.2. Ensure correspondence between the information contained in the DC and the identification details declared by the CLIENT.

3.2. Verify the certificate holder's and the CLIENT's identity, their legitimacy and sufficiency of the powers considering the documents displayed by the CLIENT.

3.3. Report to the CLIENT confirmation of the information concerning the conclusion of the contract and the acceptance of the Agreement Form, as provided in 8.4.

3.4. Ensure a unique identification element to each certificate holder of the DC, which cannot be assigned to another entity.

3.5. Maintain the elements which attest the identity and power of attorney of the certificate holder and the CLIENT for 7 years after the expiration date of the DC.

3.6. Prevent forgery or alteration of the data on the DCs.

3.7. Use reliable systems for the generation of the DCs, to ensure that:

3.7.1. The authenticity of the information may be verified;

3.7.2. Any changes of technical nature, which may affect the safety requirements, are immediately detectable.

3.8. Maintain the issued QDCs for a period of seven years, from the date on which they expired.

3.9. Revoke / suspend the DC as set forth in this 'General Terms and Conditions', pursuant to legal provisions, by decision of the Supervisory Body, or by the verification of one or more revocation reasons present in the MULTICERT`s Certificate Practice Statement.

3.10. Publish, by electronic means, the revocation or suspension of the DC.

3.11. Notify the certificate holder, by electronic means or other means, the change of status of the DC.

3.12. Observe other duties that may be imposed by regulatory provisions, or provisions set out by the Supervisory Body.

3.13. MULTICERT, under any circumstances, will intervene in the relationship between the certificate holder or the CLIENT and any third parties of this Digital Certificate Issuance Agreement.

SECTION 4 – OBLIGATIONS OF THE CLIENT AND THE CERTIFICATE HOLDER

4.1. The CLIENT is obliged to:

4.1.1. Respect, and enforce, by the certificate holder who has legitimate access to the DC, all the provisions established in this General Terms and Conditions.

4.1.2. Provide complete and accurate documentation and information on the personal and professional data of the certificate holder.

4.1.3. Notify MULTICERT of all subsequent changes concerning the client's identification and/or change of other features influencing the attributes of the DC and the date in which it occurred.

4.1.4. Notify MULTICERT, as soon as possible, of any fact likely to cause direct or indirect damages, to the own or a third party, namely of all and any use of its private key outside the scope of this agreement.

4.1.5. Pay the price of the services provided by MULTICERT.

4.2. The certificate holder is obliged to:

4.2.1. Use the DC exclusively in accordance with this 'General Terms and Conditions', according to its intended aim and in the scope of the corresponding Certificate Policy and Certificate Practice Statement available at https://pki.multicert.com/.

4.2.2. Use the DC exclusively in the quality or power of attorney for which the DC was issued.

4.2.3. Verify personal data concerning him and which are recorded in the DC and communicate to MULTICERT all the inaccuracies which may be found.

4.2.4. Notify MULTICERT of all subsequent changes concerning his identification and/or change of other features which influence the attributes of the DC; and the date on which it occurred.

4.2.5. Notify MULTICERT of all the documentation which had expired and provide the new valid, complete and accurate documentation, whenever the certificate holder wishes to renew the DC within the scope of the simplified renewal foreseen for the first and second years of the validity period of the DC after its issuance date.

4.2.6. Notwithstanding the provisions of the previous paragraph, ensure that the private key is kept under the certificate holder's control and that adequate measures are taken to prevent its unauthorized use during its validity period, ensuring, for this purpose, the appropriate mechanisms of physical, procedural and technical security.

4.2.7. Ensure that the DC access code remains safe, confidential and only accessible by the certificate holder. In the case of Remote / Cloud QDC this condition extends its applicability to the OTP code.

4.2.8. Not disclose or make available to third parties, the identification parameters and procedures of that private key.

4.2.9. Be equipped with computer systems and applications or electronic services which comply, in terms of hardware and software, with the technical requirements for installing the DC, or the private key, and the usage of the DC.

4.2.10. Not use a private key whose DC is suspended, expired, or revoked.

4.2.11. Request to MULTICERT the immediate suspension and/or revocation of a DC, whenever there is the suspicion of breach of confidentiality of the private key or whenever it is verified one of the suspension/revocation reasons constant in the Certificate Practice Statement, following the revocation process made available by MULTICERT.

4.2.12. Destroy the private key if, after being lost and even if it was revoked, the same is found.

4.2.13. Notify MULTICERT, as soon as possible, of any fact likely to cause direct or indirect damages, to the own or a third party, namely of all and any use of its private key outside the scope of this agreement.

4.2.14. In the case of collection in person of the QDC, collect it up to 30 days after its issuance, otherwise the QDC will be revoked as stated in section 9, and MULTICERT may not make any refund of the amounts already paid. This is not applicable to the Remote/Cloud QDC.

SECTION 5 – Digital Certificates (DCs)

5.1. CONTENT OF DCs

5.1.1. The DC issued by MULTICERT contains all the requirements which this assumes as necessary, not disregarding all the legal obligations to which it is subject.

5.1.2. The CLIENT acknowledges that the DC does not contain any information other than the mentioned in the preceding paragraph.

5.1.3. Furthermore, by request of the CLIENT, the DC may contain other information, namely regarding pseudonyms, powers of attorney granted to the certificate holder by third parties, academic titles, professional qualifications or other attributes, provided that it falls within the scope of the Certificate Policy related to the DC.

5.1.4. If the elements mentioned above are not proven to MULTICERT, this may not issue the DC.

5.2. USE OF THE DC AND PROBATIVE VALUE

5.2.1. The obligations assumed by the certificate holder and by the CLIENT, concerning the use of a QDC during its validity period, remain valid after it expires.

5.2.2. The probative value of the electronic documents to which was affixed an electronic signature using the QDC, as provided by this 'General Terms and Conditions', is provided by article 25º of the Regulation (EU) No 910/2014 of the Parliament and of the Council.

5.3. RENEWAL OF DCs

5.3.1. If the certificate holder wishes to continue using the certificate for longer than agreed and if the purposes for which the certificate was issued are the same, it will only be required to pay for the renewal, by following the instructions which will be sent by MULTICERT to the e-mail address indicated in the field E-mail Address, and if MULTICERT does not acknowledge receipt thereof, within the established deadline, it will assume that the certificate holder does not intend to carry out the renewal and will revoke the certificate, which ceases to be valid. This procedure will only be valid for the first and second year. When the digital certificate reaches 3 years of validity, the renewal process will require the delivery of a new form and new documentation. This procedure is not applicable to the TLS/SSL digital certificates, in which case the digital certificate renewal will always oblige the delivery of new form and documentation.

5.4. SUSPENSION OF DCs

5.4.1. The certificate holder agrees to suspend the DC through electronic channel available 24/7, whenever there are sufficient reasons for that. Alternatively MULTICERT shall suspend the DC, within no more than 24 hours (on business days), after the reception of the certificate holder's notice or notice by MULTICERT, in the following circumstances:

5.4.1.1. Upon written request of the certificate holder, sent to MULTICERT by fax or electronic mail digitally signed with the private key corresponding to the DC.

5.4.1.2. Whenever there are sufficient reasons to consider that a DC was issued based on erroneous or false information, that the information no longer corresponds to reality, or when there is suspicion that the confidentiality of the private key was breached.

5.4.1.3. In compliance with the decision of a judicial authority, or notification of a police force.

5.4.2. The suspension of the DC is always notified, by electronic means, to the certificate holder, and immediately inscribed in the certificate register, notwithstanding the subsequent withdrawing of the suspension.

5.5. REVOCATION OF DCs

5.5.1. The time elapsed between the revocation request and its disclosure will not take more than 24h.

5.5.2. MULTICERT will revoke the DC in the following circumstances:

5.5.2.1. Within 30 days, if the certificate holder does not perform the provisions in paragraph 4.2.14.

5.5.2.2. Upon request of the certificate holder:

5.5.2.2.1. By submission of the web revocation form, or

5.5.2.2.2. By filling in the revocation form, which shall be sent to MULTICERT by mail, digitally signed e-mail, or delivered directly at MULTICERT's premises.

5.5.2.3. After confirming the inconsistency of the information provided and/or contained in the certificate and which caused the suspension of the DC, in accordance with paragraph 5.4.1.2.

5.5.2.4. Whenever the confidentiality of the private key is breached.

5.5.2.5. In the case MULTICERT ceases activity.

5.5.2.6. By order of the Supervisory Body or by court decision.

5.5.2.7. In case of death, disability or incapacity of the natural person, or the extinction of the collective person holder of the DC, when it has knowledge of such events.

5.5.2.8. In case the annuity is not paid within the maximum period of 30 days after the payment due date, when it is agreed the payment of the price in annual installments. Not applicable to TSL/SSL and PSD2 certificates.

5.5.2.9. In case of verification of one or more reasons for revocation contained on the MULTICERT Certification Practice Statement.

5.5.2.10. MULTICERT will proceed to the revocation of the DC when requested by the certificate holder and based on the information provided by the certificate holder, respecting the revocation process of MULTICERT.

5.5.2.11. The revocation of the DC will be always communicated, by electronic means, to the certificate holder. The communication of the decision of revocation of the DC based in 5.5.2.3**Erro! A origem da referência não foi encontrada.**, 5.5.2.5**Erro! A origem da referência não foi encontrada.**, 5.5.2.6**Erro! A origem da referência não foi encontrada.** will always be founded, as well as immediately inscribed.

5.6. EFFECTS OF SUSPENSION, REVOCATION AND TERMINATION

5.6.1. The suspension and revocation of the DC are enforceable against third parties, from the date and time of their publication by MULTICERT, in computer record for online query, unless if it is proved that its cause was already acknowledged by the third party, remaining outstanding only the obligations outstanding prior to the mentioned registration.

5.6.2. The suspension or revocation of the DC prevents the issuance, by MULTICERT, of another DC concerning the same key pair.

5.6.3. A revoked DC cannot be reused.

SECTION 6 – CONCLUSION OF THE AGREEMENT AND DCs ISSUANCE AND VALIDITY PERIOD

6.1. CONCLUSION OF THE AGREEMENT AND ISSUANCE TIME OF THE DC

6.1.1. The issuance request is considered to be concluded on the date in which the Agreement Form is accepted by MULTICERT (or by MULTICERT's Registration Authority), which shall occur within 5 business days after MULTICERT (or MULTICERT's Registration Authority) has received the original form, duly completed and signed by the CLIENT.

6.1.2. Upon acceptance of the Agreement Form, MULTICERT will issue the DC, the corresponding asymmetric key pairs, or will provide the technical means necessary to the creation of those key pairs.

6.2. VALIDITY PERIOD AND TERMINATION OF THE AGREEMENT

6.2.1. The DC issued by MULTICERT is valid for the period mentioned in the Agreement Form from the date of its issuance and other services related to the digital certification will be provided for the same period, unless in the meantime another period is agreed, which cannot, however, exceed 3 years. In case of SSL/TLS certificates the validity cannot exceed 2 years.

6.2.2. MULTICERT does not support the practice of renewal of certificates, considering it a reissuance, i.e., a renewal will lead to the generation of a new key pair. Thus, the certificate holder shall request the reissuance of the DC up to 8 days before the current certificate expires, relying on the certificate issuance process used previously. Not applicable to TLS/SSL and PSD2 certificates.

6.2.3. Termination of the DC causes termination of this agreement.

6.2.4. The maximum period of validity for using the private key is 3 years. In case of TLS/SSL certificates, the maximum period of validity for using the private key is 2 years. Upon renewal, which shall occur before reaching this period, the key pair is not reused, so a new key pair is always generated.

6.2.5. Before reaching the maximum period of validity of the DC and still under this Digital Certificate Issuance Agreement, MULTICERT will notify the certificate holder to present, once more, the documents required for the issuance of a DC, after which it will issue a new DC (with generation of a new key pair) according to the validity period referred in the Agreement Form.

SECTION 7 – PURCHASE THROUGH AUTHORIZED AGENTS

7.1. If the CLIENT purchased the DC from a MULTICERT authorized agent, to the binding between MULTICERT and the CLIENT will apply the present General Terms and Conditions, with the following adjustments:

7.1.1. The certificate holder agrees to notify the agent to whom he has acquired the DC, as provided in paragraphs 4.2.4, 4.2.7**Erro! A origem da referência não foi encontrada.**, unless this is no longer a MULTICERT authorized agent.

7.1.2. The obligation to pay the price as foreseen in paragraph 4.1.5 has to be fulfilled by the CLIENT before the authorized agent, if such is agreed with that agent.

7.1.3. The issuance of the DC as provided in Section 10 must be requested to the authorized agent.

7.2. The provisions in this section do not imply transfer to the agent of any of the functions of MULTICERT as a certification authority, the agent has no role in that activity, as a registration authority or other.

SECTION 8 – DC ISSUANCE PROCESS

8.1. The CLIENT may request the DC issuance by accessing MULTICERT's website, by contacting directly MULTICERT or any MULTICERT's Registration Authority, or through an Authorized Agent.

8.2. MULTICERT may refuse the issuance of a DC if, according to its internal procedures, it verifies that the certificate holder does not comply with the requirements deemed necessary to install the DC, namely for lack of appropriate hardware and software, or lack of integrity.

8.2.1. In the case provided in the previous paragraph, MULTICERT will notify the CLIENT, by electronic means, of it not accepting the Agreement Form for concluding the contract.

8.2.2. Refusal to issue a DC does not grant the CLIENT the right to recover the amounts paid, whenever it results from causes not attributable to MULTICERT.

8.2.3. In particular, the certificate holder will not have the right to a reimbursement of the amounts paid if it is established that he has provided erroneous or false information, or that he has omitted information or documentation considered relevant for examining the request and which MULTICERT would need for that issuance.

8.2.4. MULTICERT may, still, decline to issue a DC, whenever the contract of a CLIENT presents erasures which may raise doubts on the identification of the certificate holder, the powers conferred to him or that somehow suggest that the contract has been changed after being signed by the CLIENT.

8.3. The CLIENT who does not present all the documentation and/or information demanded for the issuance of a DC will be notified by MULTICERT, by electronic means, to do it in a maximum period of 40 days.

8.3.1. The issuance, in this case, will only proceed after the CLIENT presents the documentation and/or provides the information, in writing, to MULTICERT, within the aforesaid period for the purpose.

8.3.2. MULTICERT may suspend the issuance of the DC whenever the CLIENT does not provide the missing documentation and/or information in a maximum period of 40 days, after having been notified for that end.

8.3.3. After the suspension of the issuance of the DC, the CLIENT may, still, continue the issuance request, by paying a reactivation fee for this purpose.

8.3.4. In the case the CLIENT does not request the prosecution of the suspended request or fails to pay the reactivation fee, the DC will not be issued, and the CLIENT will not

have the right to recover the amounts paid.

8.4. Upon communication to the CLIENT, by MULTICERT (or MULTICERT's Registration Authority), that the information concerning the agreement was verified, as established in 3.3, it is given notice of the acceptance of the Agreement Form.

SECTION 9 – PRICE OF THE DC ISSUANCE AND PAYMENT METHOD

9.1. The price for the issuance and reactivation of the DC issuance request, as well as the corresponding payment methods, are indicated by MULTICERT or by other entity appointed by it (Registration Authority or authorized agent).

9.2. The price for the issuance of the DC may be augmented, in terms to be indicated by MULTICERT, by the Registration Authority or authorized agent, whenever it is requested to MULTICERT, during the certificate issuance process, to change it in a way that implies reissuing a certificate already issued or reassessing the documentation which supports its issuance.

SECTION 10 – CONFIDENTIALITY AND AUTHORIZATION FOR DATA PROCESSING AND TRANSMISSION, IF THE TITLEHOLDER IS A NATURAL PERSON

10.1. MULTICERT agrees to ensure secrecy and confidentiality of all personal data whose knowledge is not intended to public disclosure, namely those concerning the private key, or other whose confidentiality may be enforced by legal or regulatory means.

10.2. The certificate holder, from this moment, expressly consents that, during the validity of this agreement and for its purposes, the personal data transmitted is subject to computer use and processing.

10.3. The data collected are intended to the issuance of the DC and compliance with other legal obligations to which MULTICERT is obliged and are not used for any other purposes, different from those mentioned. It is considered included in the purposes mentioned the use of the contacts of the certificate holder or CLIENT for the purpose of satisfaction surveys with the services provided by MULTICERT.

10.4. The certificate holder expressly consents the personal data required to execute the Digital Certificate Issuance Agreement to be collected by MULTICERT, or by the CLIENT, and expressly agrees and consents that, in the scope of this agreement, MULTICERT is responsible for processing personal data; the certificate holder further consents MULTICERT to subcontract third parties for the processing of such data; MULTICERT is obliged to ensure observance, by the entities subcontracted, of the purposes for which the data is collected.

10.4.1. Any right of the certificate holder regarding the matter of this Section may be exercised, in writing, to the address indicated in 15.6.1.

10.5. All fields of the Agreement Form are required fields, under penalty of not being able to access to MULTICERT services, and the personal data to be included shall be directly provided by the certificate holder.

10.6. MULTICERT agrees to keep up to date the certificate holder's personal data which is communicated, updating it whenever deemed necessary and taking appropriate measures to ensure that inaccurate or incomplete data is deleted or amended.

10.7. The certificate holder may, at any time, access his personal data, held by MULTICERT, and may require its modification or deletion, provided that such does not conflict with the legal requirements to which MULTICERT is obliged.

10.8. The certificate holder may request his personal data which is inaccurate, incomplete, outdated, or whose collection, use, communication or retention are forbidden, to be rectified, completed, clarified, updated or suppressed.

10.9. In case the certificate holder demands the suppression of information which MULTICERT finds necessary to provide the services which are object of this agreement, MULTICERT may cease to provide the service and terminate the Digital Certificate Issuance Agreement, wherein the CLIENT does not have the right to indemnification or a reimbursement of the amounts paid.

10.10. The certificate holder accepts and authorizes MULTICERT to communicate to a third party his personal data, including name and address, if this communication is reasonably necessary under some legal requirement or regulation, as well as to comply with any requirement of a judicial or administrative authority, and any other lawful purpose, as provided by article 6 of the Regulation (EU) 2016/679 of the Parliament and of the Council.

10.11. In the case MULTICERT assigns to a third party the rights and obligations arising from this agreement, it is obliged to take measures with the certificate holder to obtain consent for the transfer of information concerning personal data and the DC.

10.12. By terminating the services provided by MULTICERT, whether due to revocation, or termination of the DC, or any other reason, the data related to the certificate holder is kept and archived confidentially by MULTICERT, for a period of 7 years after the expiration date of the DC, according to requirement 6.4.6 of ETSI EN 319 411-1, Regulation (EU) 910/2014 of the Parliament and of the Council of 23 July.

SECTION 11 – INTELLECTUAL PROPERTY RIGHTS

11.1. The CLIENT hereby acknowledges that the issuance of the DC is based on computer programs and that processing of personal data and, also, personal data included on the DC, is compiled in computer databases.

11.2. The CLIENT expressly recognizes that the computer programs and databases mentioned in the previous paragraph are protected by copyright, trademark, patent and any other intellectual or industrial property right which is granted thereto according to the current laws.

11.3. The CLIENT also acknowledges that MULTICERT is the only holder of the rights mentioned in the previous section and, also, any rights on the content of databases.

SECTION 12 – AMENDMENT TO THIS AGREEMENT

12.1. If, during the validity of this agreement, new laws or new regulations of existing legislation are published, which concerns terms comprised in this General Terms and Conditions and which impose amendment to the fundamental obligations of the parties, and still, if MULTICERT comes to realize that it shall amend the terms of the Certification Practices Statement and the Certificate Policy of the type of digital certificates which had been defined and/or agreed, this General Terms and Conditions shall be amended accordingly.

12.2. MULTICERT shall communicate to the CLIENT the new text of the agreement, which is considered to have been accepted by the CLIENT if this expressed its acceptance, or did not object to its content within 30 days after that communication.

12.3. If the CLIENT communicates to MULTICERT the non-acceptance of the suggested amendments and consensus not being possible, any of the parties will have the power to terminate this agreement; such termination taking effect sixty days after notifying the other party to that end.

SECTION 13 – LIABILITY

13.1. MULTICERT is only liable under civil law for loss or direct damage caused to the CLIENT or third parties in the case of breach of all or part of its obligations resulting from this 'General Terms and Conditions', when guilty of intentional fault or gross negligence.

13.2. MULTICERT is not responsible for the certificate holder's use of the corresponding DC if this is improper, or contrary to this 'General Terms and Conditions' and the legal provisions and regulations which govern its issuance and use.

13.3. Similarly, MULTICERT is not responsible for the use of the programs for generation of the key pair and DC issuance request, namely if the certificate holder's computer system has any computer virus which may affect that issuance and use.

13.4. The certificate holder is civil and criminal responsible for any act which breaks this 'General Terms and Conditions' and, particularly, for his use of the private key corresponding to the DC.

13.5. The CLIENT is responsible for the accuracy of the data and information provided under the scope of this Agreement.

13.5.1. The certificate holder is responsible for the actions carried out by anyone using the private key corresponding to the DC.

13.6. The certificate holder accepts and acknowledges that the entry, navigation, communication exchange and subscription of MULTICERT's services are his sole responsibility; MULTICERT cannot be sued for damages incurred to the certificate holder or by third parties which may occur by using the service, including contamination by computer virus, except if such damage results from intentional fault or gross negligence on the part of MULTICERT.

SECTION 14 – WITHDRAWAL OR TERMINATION OF THE AGREEMENT

14.1. ON WITHDRAWAL

14.1.1. The CLIENT may withdraw the CONTRACT at any time upon prior notice sent at least 60 days before the date on which it takes effect.

14.1.2. Exercising the option provided in the preceding paragraph will not grant the CLIENT the right to receive any reimbursement from MULTICERT of the amounts already paid.

14.2. ON TERMINATION

14.2.1. Given the nature of the issuance of the DC, namely as it consists of providing a good, created according to the specifications of the certificate holder and as it is manifestly customized, the CLIENT expressly acknowledges having no right to freely terminate the contract.

14.2.2. Any of the parties may terminate this agreement, with immediate effect, if the other party fails seriously or repeatedly to comply with its contractual obligations, as well as if there are circumstances which render impossible or severely undermine the attainment of the contractual purpose.

14.2.3. For the purposes of the preceding paragraph, the parties mutually accept the following:

14.2.3.1. Breach is any non-compliance with this agreement, in the whole or in part, from which results damage to the non-defaulting party;

14.2.3.2. The breach of the obligations of the parties involving breach of the rules concerning the use of the DC, private key tampering, the infringement of intellectual property rights, or the breach of data confidentiality will always be considered serious breach of contract;

14.2.3.3. The breach of any obligations under this agreement which is repeated after the non-defaulting party having requested its compliance to the other party, in writing, within a period of 15 days, will be considered repeated non-compliance.

14.2.4. If MULTICERT terminates this agreement, the CLIENT is not exempted from payment of the amounts due at the time of termination, and MULTICERT does not have to return any amounts already received.

14.2.5. Termination of contract becomes effective upon notice to the counterpart, granting the non-defaulting party the right to compensation for all damages it had suffered.

14.3. REVOCATION

14.3.1. In the cases specified in 12.3, 14.1.1, 14.1.2, MULTICERT will revoke the corresponding DC, and will immediately give notice that the DC is revoked within no more than 24 hours, from the time at which the notice comes into effect.

14.3.2. Upon revocation of the DC, the certificate holder will refrain from using the DC to sign any electronic document and, when the support corresponding to the DC enables this, it will be destroyed.

SECTION 15 – FINAL PROVISIONS

15.1 The CLIENT declares having been informed of the technical options to get evidence of the sending and receiving of digitally signed messages.

15.2 The CLIENT must not assign to a third party any rights or obligations under this agreement, except with the consent of MULTICERT.

15.3. Any changes to this General Terms and Conditions shall take the form of written addendum to the agreement, signed by both parties.

15.4. Regardless of any provision of this General Terms and Conditions being considered illegal or unenforceable, void, null or declared ineffective, the remaining provisions shall remain valid and shall take effect; the parties undertake to agree a new provision, free from these defects, which will produce the same effects intended by the parties as the invalid provision.

15.5. When there is an occurrence considered as a case of force majeure which prevents the timely fulfillment, by either party, of its obligations within the deadlines set, the deadline for that compliance will be delayed for the period corresponding to the resulting delay, notwithstanding all possible efforts made by the parties to minimize its consequences.

15.5.1. The party wishing to invoke an event of force majeure, as soon as it is aware of it, shall give notice, in writing, to the other party, providing, immediately, evidence of the event invoked and indicating its impact on Contract execution.

15.5.2. When the force majeure event definitely prevents compliance with the Contract, by either party, it can be terminated by any of them, this not resulting in compensation for non-compliance, notwithstanding the debts which may exist to date. It is considered that there is a permanent impossibility of compliance, namely when the impossibility continues for more than 90 days.

15.6. Any notice or communication to any of the parties, under this agreement, shall be carried out in writing and can be delivered to the counterpart, or sent by express mail, or through transmission by e-mail, digitally signed, or by telefax, to the address indicated below (or to any other address or number which for the purpose may have been opportunely notified by the corresponding party).

15.6.1. Notices or communications referred to in the previous paragraph shall be addressed as follows:

To MULTICERT:
- e-mail: info@multicert.com, for subjects related to data privacy: privacy@multicert.com
- telefax: +351 217 123 011
- address: Lagoas Park, Edifício 3, Piso 3 – 2740-266 Porto Salvo – Oeiras - Portugal

To the CLIENT: according to the information inscribed in the Agreement Form of this contract. Notices concerning financial matters will be sent to the e-mail addresses of the financial contact indicated in the Agreement Form.

15.6.2. Any of the parties may change, whenever it deems it appropriate, the address, the e-mail address and the number of telefax to which communications shall then be addressed, by written notice sent to the other party, two business days before.

15.6.3. Communications or notices will be considered as having been regularly carried out if their recipient did not communicate previously to the other party, under the terms set, to have changed its addresses.

15.6.4. Except if proven otherwise, the referred notices and communications shall be considered as having been received or performed and delivered, in the case of letters, five business days after its dispatch by mail; in the case of delivery with protocol, when being delivered in the corresponding address; and in the case of e-mail or telefax, after acknowledgement from the recipient or the business day after the receipt.

15.7. The headings of the sections of these agreement terms are merely indicative and cannot be interpreted as a change or modification, in any way whatsoever, of the provisions contained herein.

15.8. If any of the provisions of this General Terms and Conditions is considered illegal, by a legal or regulatory provision, current or future, or by a judicial decision with res judicata, issued by a Court or other competent body, such provision shall be considered as not written. All other provisions of this agreement keep binding force.

15.9. Except as provided otherwise, failure by any of the parties to exercise any of the rights or powers granted to them by this General Terms and Conditions, can in no case mean a waiver to such right or power or lead to its expiry, so it will remain valid and effective despite not being exercised.

SECTION 16 – DISPUTE RESOLUTION AND GOVERNING LAW

16.1. In case of dispute, the consumer may resort to an Alternative Dispute Resolution Entity. The official List of such Entities is available on the Consumer Website at www.consumidor.pt.

16.2. Notwithstanding the possibility of prior use of mediation, if no agreement is reached between the parties under that procedure for any dispute arising out of the interpretation, application or execution of this agreement, either party may resort to legal proceedings, being set as competent jurisdiction for the purpose the District Court of Lisbon.

16.3. To this Digital Certificate Issuance Agreement shall apply the Portuguese Law.

September 16, 2019