TERMS AND GENERAL CONDITIONS OF THE ELECTRONIC CERTIFICATION SERVICE

DEFINITIONS APPLICABLE TO THE AGREEMENT

AGREEMENT: all the contractual documentation, these General Terms and Conditions, the Certification Practices Statement applicable to the contracted service and other documents that govern the relations between the Parties.

CERTIFICATION PRACTICES STATEMENT or CPS: a set of practices adopted by a Certification Authority for the issue of certificates that contains detailed information about their security, support, administration and Certificate issue system, and on the trust relationship between the Parties. They are published on CAMERFIRMA's website https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/

AC CAMERFIRMA SA (hereinafter, CAMERFIRMA): Trust Service Provider (TSP), of Spanish nationality with headquarters in Madrid, Calle Ribera del Loira 12, with Tax ID No. A-82743287, telephone 902550304/913443743 and e-mail address info@camerfirma.com, which is subject to the statutory supervision of the Ministry for the Economy and Business (formerly dependent on the Ministry for Energy, Tourism and Digital Agenda). CAMERFIRMA provides trust services pursuant to EU Regulation 910/2014, 23 July 2014 and ETSI standards EN 319 401; ETSI EN 319 411-2; ETSI EN 319 421, pursuant to its Conformity Assessment Reports prepared by an accredited conformity assessment body, which can be found on its website: https://www.camerfirma.com/camerfirma/acreditaciones/. In the provision of the service requested, CAMERFIRMA acts as Certification Authority (hereinafter, the "CA") relating a specific public key to a specific person or entity by issuing a Digital Certificate.

REGISTRATION AUTHORITY (hereinafter, the RA): the entity responsible, among other functions, for verifying the APPLICANT's identity and, if applicable, of the other circumstances associated with the certificate, pursuant to Section 1.3.2 of CAMERFIRMA's eIDAS CPS. All or part of the functions of RA may be assumed either directly by CAMERFIRMA, or by a delegated RA (Chamber of Commerce RA, Corporate RA, etc.).

The APPLICANT: a natural person who requests the issue of a certificate for him or herself (with or without a representation relationship or corporate connection to an ENTITY), in which case he or she assumes the status of CERTIFICATE HOLDER/SIGNATORY (electronic signature certificates), or for an ENTITY in which case it is the ENTITY that assumes the condition of CERTIFICATE HOLDER/SUBSCRIBER (component certificates). In all cases, the APPLICANT is responsible for the certificate.

The ENTITY: the organisation with or without legal status linked to the CERTIFICATE HOLDER/SIGNATORY of a certificate through a representation relationship or corporate relationship, or the CERTIFICATE HOLDER/SUBSCRIBER of the Certificate in the case of component certificates issued to organisations.

QUALIFIED CERTIFICATE: Qualified electronic certificate of signature , electronic seal, website authentication or timestamp (depending on the trust service contracted) issued by a Qualified Trust Service Provider pursuant to EU Regulation 910/2014, 23 July 2014 ("eIDAS" regulation) and that appears on the Trust Lists (TSL).

QUALIFIED CERTIFICATE FOR ELECTRONIC SIGNATURE: An electronic signature certificate that has been issued by a qualified trust service provider and that meets the requirements established in Appendix I of the eIDAS Regulation, offering the maximum legal guarantees regarding the identification of the signatory and the signatory's connection with the electronic signature, guaranteeing the uniqueness, integrity and non-repudiation of the data that is linked to the signature.

QUALIFIED CERTIFICATE FOR ELECTRONIC SEAL: an electronic seal certificate that has been issued by a qualified trust service provider and that meets the requirements established in Appendix III of the eIDAS Regulation, offering the maximum legal guarantees regarding data integrity and correctness of the origin of that data to which the qualified electronic seal is linked.

QUALIFIED CERTIFICATE FOR COMPONENT: a component certificate that has been issued by a qualified trust service provider and that meets the requirements of the eIDAS Regulation for each type (eIDAS Appendix III and IV), enabling unattended signature and authentication between computer components in automated processes (electronic seal for automated processes) or the authenticity of the Entity/Organisation that owns the website (SSL).

UNQUALIFIED CERTIFICATE: a certificate of electronic signature, seal or component that has been issued by a trust service provider (qualified or not) that meets the requirements established in EU Regulation 910/2014, 23 July 2014 ("eIDAS" regulation) for each corresponding trust service, but which has not been subject to a prior conformity assessment and is not included in the trust lists (TSL). Unqualified certificates offer technical and legal guarantees similar to qualified certificates, except for the onus of proving the provider's intentionality or negligence, which falls upon the damaged user, and except where documents/data that do not apply for unqualified services are presumed to be valid.

SECTION I
TERMS AND CONDITIONS APPLICABLE TO ALL TYPES OF CERTIFICATES

1. PURPOSE

The issue by the CA in favour of the APPLICANT of a digital Certificate of the type that appears in the application form and the conditions of use by the APPLICANT of the Digital Certification Service, pursuant to the terms provided within this agreement, the eIDAS Regulation and local laws.

2. LEGAL FRAMEWORK FOR THE SERVICE PROVISION

The APPLICANT declares to know the Certification Practices Statement (CPS) and Certification Policies (CPs) applicable to the contracted service, which are available on CAMERFIRMA's website (www.camerfirma.com). The terms and conditions of this document, together with CAMERFIRMA's Certification Practices Statement (CPS) and the CPs, constitute the legal framework that shall regulate the relationship between the parties, internally and with third parties, without prejudice to the provisions of current law. This document is therefore a summary of the most relevant rights and obligations.

3. AGREEMENT DURATION

This agreement will enter into force and will end coinciding with the issue and expiry dates indicated in the contracted Certificate, without prejudice to the causes for revocation provided for in the CPs and CPS, and may be renewed pursuant to the terms established in the CPS.

4. PAYMENT

The price of the Certificate, which shall include payment for the services associated with it provided by CAMERFIRMA, is defined in the offer that the APPLICANT or the ENTITY formalised when applying for the Certificate and on the corresponding invoice.

This price must be paid by the APPLICANT or the ENTITY, to the CA or RA, prior to the issue of the Certificate, unless otherwise agreed in the offer.

5. ACCEPTANCE OF THE CERTIFICATE

The APPLICANT expressly accepts the certificate, confirming and accepting the accuracy of its content, with the consequent obligations derived from these before the RA, CA or any third party that in good faith places its trust in the content of the Certificate, in virtue of the CPS and/or current law. If there is any discrepancy between the data provided to the CA and the content of the Certificate, or if an error is detected, the CA must be immediately notified by the APPLICANT or the ENTITY so that the Certificate can be revoked.

6. THE CA'S OBLIGATIONS

a) Communicate to the APPLICANT or the ENTITY the revocation or suspension of his or her Certificate or the certificate for which he/she is responsible, if applicable, explaining the reasons and the date and time from which the certificate will no longer be effective pursuant to the procedures defined in the CPS. For security reasons, the CA may revoke a certificate unilaterally and immediately without the CERTIFICATE HOLDER claiming any compensation due to this revocation. CAMERFIRMA will replace the certificate with a valid one provided that the anomaly is corrected.
b) Keep the database of valid Certificates, suspended Certificates and revoked Certificates up-to-date.
c) Process the requests for suspension/revocation of Certificates as soon as possible.
d) Correctly identify the APPLICANT through the RA, pursuant to the procedures established in the CPS.
e) If applicable, check the information regarding the ENTITY's incorporation and legal status and the APPLICANT's representation relationship or corporate relationship with it, pursuant to the procedures established in the specific CPs for this type of Certificate.

f) Archive and conserve information regarding the data issued and received for 15 years. This information may be archived digitally.
g) Issue the Certificate to the APPLICANT, through the RA, pursuant to the conditions defined in the CPS, once the prior checks have been completed.
h) All obligations derived from the content of the specific CPS, as well as in current law.

7. THE APPLICANT AND THE CERTIFICATE HOLDER/SIGNATORY'S OBLIGATIONS:

a) Keep the Certificate and the private keys*, passwords and pin numbers safe in a diligent manner, taking reasonable precautions to avoid their loss, disclosure, modification or unauthorised use.
b) Request the suspension/revocation of the Certificate in the event of any Certificate suspension or revocation incident provided for in the CPS and in current law.
c) Not to reveal the private key or its activation PIN.
d) Supply all the information and documentation requested, being responsible for its accuracy and correction.
e) Immediately notify the CA if any incorrect or inaccurate information is detected, or if, unexpectedly, the information on the Certificate does not match.
f) Immediately inform the CA about any situation that may affect the validity of the Certificate, or the security of the keys.
g) Use the Certificate pursuant to the Law and the limits established by the CPS and the Certificate itself depending on the type.
h) Any other derived from the content of the CPS in relation to each type of certificate.

**Custody of the Certificate and its private key does not apply to remote certificates since the CA is responsible for its custody.*

8. THE ENTITY'S OBLIGATIONS

The APPLICANT's obligations b), d), e), f), g) and h) also apply to the ENTITY, and may be exercised through its legal representative.

9. LIMITS OF USE ACCORDING TO THE PURPOSE OF THE CERTIFICATE

Each type of electronic certificate is intended for a specific person (natural person, legal entity or entity without legal status) and is for the purpose of certain functions that are defined in the CAMERFIRMA's CPS in the descriptive sections of their hierarchies. Insofar as the certificates may contain the CERTIFICATE HOLDER's specific attributes, the RA completes the necessary verifications that enable these attributes to be authentically certified (representation relationship, corporate relationship, affiliation, etc.) prior to its issue. In the case of electronic signature certificates with an entity representation attribute, the certificate references the document on the basis of which it has been accredited to the RA that the powers of representation of the CERTIFICATE HOLDER/SIGNATORY conform to the purpose of the certificate. However, the correct use of the certificate according to its purpose and the powers of representation that have been granted is the responsibility of the CERTIFICATE HOLDER/SIGNATORY and it is the responsibility of trusting third parties to verify the purpose of the certificate and any limitations of its use.

10. THE USE OF THE CERTIFICATE FOR COMMERCIAL PURPOSES IS STRICTLY PROHIBITED

The contracting of the CAMERFIRMA Digital certification service solely allows for the use of the Certificate in the field of activity of the APPLICANT or of the ENTITY, pursuant to the purpose of the type of certificate requested. Once the certificate has been issued, unless specifically agreed otherwise between the parties, the APPLICANT or the ENTITY may not use the Certificate for commercial purposes. Commercial use of the certificate is understood as any action by means of which the APPLICANT or the ENTITY offers third parties outside of this Agreement, whether for a consideration or free of charge, services that require the use of the Certificate issued.

Breach of this condition shall empower the CA to revoke the certificate and claim compensation for damages and losses caused by the breach, including loss of potential profit and indirect damages.

11. RIGHT OF WITHDRAWAL (only applies to APPLICANTS who are considered consumers pursuant to RDL 1/2007)

The issue of the digital certificate to the APPLICANT or to the ENTITY either as a download on software media or by issuing or storing on hardware media, implies the commencement of the agreement's validity, which, pursuant to the General Law for Consumers' and Users' Defence (RDL 1/2007) in such cases, the APPLICANT and the ENTITY concede their right of withdrawal.

12. RESPONSIBILITIES

The CA and, if applicable, the RA, are responsible for the functions that correspond to them according to the applicable CPS and, in particular, assume full responsibility for the correct verification of the identity of the APPLICANT and, if applicable, the ENTITY, and any other circumstances.

The CA and the RA are not responsible for the damages derived from or related with the non-implementation or defective implementation of the obligations attributable to the APPLICANT, of the ENTITY or of third party users, nor the incorrect use of the Certificates and keys, nor for any indirect damage that may result from the use of the Certificate or the information supplied by the CA, in particular, loss of potential profit, loss of income or data loss, which shall not give rise to any form of compensation.

Neither the CA nor the RA are liable to the CERTIFICATE HOLDER or to third parties for inappropriate or fraudulent use of the certificate if the CERTIFICATE HOLDER has assigned or authorised its use to another person. The CERTIFICATE HOLDER is solely responsible for the keys associated with the certificate.

Neither the CA nor the RA are responsible for possible inaccuracies on the Certificate that result from the information provided by the APPLICANT, on the condition of always having acted with the highest level of diligence.

Neither the CA nor the RA shall assume any responsibility for not implementing or a delay in implementing any obligation pursuant to the CPS if such lack of or delay in implementation results in, or were a consequence of, force majeure, act of God or, in general, any circumstance over which the CA may not have reasonable control and ,among others: natural disasters, war, state of siege, alterations of public order, transport strikes, electricity or telephone supply cuts, computer viruses, outages in telecommunication services, breaches of security in the certification system or any harm that may be derived from unforeseeable technical incidents.

Neither the CA nor the RA shall be responsible for the content of the documents that are digitally signed or encrypted.

Neither the CA nor the RA are responsible for the correct operation of applications that are not approved, or for damages resulting from impossibility of use of these applications.

Nor shall they be responsible for deterioration or faults in the computer equipment or in the data due to reasons not directly attributable to the use of the Certificates or the installation of the certificate, and whenever the APPLICANT does not act with the necessary diligence.

13. AMENDMENTS

The CA may modify this agreement by communicating to the APPLICANT when the change directly affects their rights and obligations, 15 days in advance, explaining, in any case, the reasons for such decision (the reasons must have a legal, technical, operational or Group policy basis). The APPLICANT (or a duly accredited representative of the CERTIFICATE HOLDER) may opt to either terminate the Agreement or renew it pursuant to the new terms. The APPLICANT or the CERTIFICATE HOLDER will have a maximum of 15 days from the date of this communication to inform the CA of his/her acceptance of the subrogation or changes made. However, if this period transpires and the CA does not receive written notification to the contrary from the APPLICANT or the CERTIFICATE HOLDER, the subrogation and amendments made shall be understood to have been accepted.

The CA may also modify the CPS or any of its clauses within the terms provided therein, at any time without the need to notify the CERTIFICATE HOLDER, in order to respond to the need to guarantee its adaptation to changes within the law and applicable technical standards. It is the APPLICANT and/or CERTIFICATE HOLDER's responsibility to understand and apply the provisions of the current CPS at all times, which is published on CAMERFIRMA's website.

14. SERVICE AVAILABILITY

Certificate can be applied for or their status queried 24 hours per day, 7 days per week and 365 days per year as indicated in the CPS.

15. DATA PROTECTION

As the entity responsible for the personal data provided by the APPLICANT/CERTIFICATE HOLDER when completing the application form, Camerfirma will process said data pursuant to Article 13 of EU Regulation 679/2016, with the help of hardcopy records and computer tools to ensure maximum security and confidentiality, in order to provide the electronic certification service and, if applicable, to issue the invoice for the service. You may exercise the rights contemplated in articles 15 to 22 of the GDPR by writing to dpd@camerfirma.com.

To obtain additional information regarding data protection and in particular about the purposes and methods established in the Privacy Statement regarding processing the personal data communicated to the APPLICANT/CERTIFICATE HOLDER at the time of making the request, please consult the following link https://www.camerfirma.com/aviso-legal/

16. CONTRACT TERMINATION

Breach of the conditions contained in this Agreement and/or in the CPS by any of the parties shall be cause for the termination. In such event, the non-breaching party shall have the right to terminate the Agreement with immediate effect. Breach by the APPLICANT or the ENTITY entitles the CA to revoke the Certificate, regardless of the damages and losses that may be claimed.

The CA has the right to revoke and not to renew the Certificate prior to the end of the validity period in the cases provided for in the CPS. When the revocation is unjustified, the CA may compensate APPLICANTS or ENTITIES who request this in writing within three months from the revocation date. This compensation may be no higher than the amount the APPLICANT paid to obtain the aforementioned Certificate.

The APPLICANT or the ENTITY may freely terminate this Agreement at any time by means of written notification with 30 days' prior notice. Under no circumstances shall this termination entitle the APPLICANT to a refund for the amounts paid to obtain the Certificate.

If the exercise of the rights of opposition or cancellation of personal data hinders the provision of services under this agreement, CAMERFIRMA shall be empowered to terminate this agreement.

17. LAW AND JURISDICTION

All matters relating to drafting, formalising and signing this agreement are governed by the laws of the country in which the consumer or entity has its principal establishment or residence.
Interpretation, execution and any other obligation that may arise after formalising and signing this agreement shall be governed by the Spanish Law that regulates the service that the consumer or the entity has contracted pursuant to the applicable European standard on electronic certification and signatures.

For the resolution of any conflict that may arise in relation to this agreement, the parties, renouncing any other jurisdiction that may correspond, submit to the jurisdiction of the Courts of the City of Madrid (Spain). If the CERTIFICATE HOLDER is a consumer, the Judge or Court that corresponds to the domicile of the consumer shall be competent.

Applies only to remote certificates

SECTION II
TERMS AND CONDITIONS APPLICABLE TO
REMOTE ELECTRONIC SIGNATURE AND ELECTRONIC SEAL CERTIFICATES

18. SCOPE The eIDAS Regulation regulates the possibility of entrusting the devices for creating electronic signatures/seals to a third party, provided that the appropriate procedures and mechanisms are applied to guarantee that the signatory has exclusive control over the use of his/her creation data for the electronic signature/seal and that the use of the device meets the requirements of the qualified electronic signature/seal (recital 51). This enables the creation of remote electronic signatures in an electronic signature/seal creation environment managed by a trust service provider on behalf of the signatory, for which specific management and administrative security procedures are applied and reliable systems and products are used, including secure electronic communication channels, to ensure that the electronic signature creation environment is reliable and used under the signatory's exclusive control (Recital 52).

19. OTHER OBLIGATIONS OF THE CA

a) The CA should apply specific management and administrative security procedures and use reliable systems and products, including secure electronic communication channels to ensure that the electronic signature creation environment is reliable and used under the sole control of the signatory. In any case, the CA's guarantee in this regard is limited to the correct functioning of the remote signature/seal procedure according to the service level contracted.
b) The CA shall safeguard the signature/seal creation data in the signatory's name and protect it against any alteration, destruction or unauthorised access, as well as guarantee its continuous availability for the SIGNATORY.
c) Due to its technical and usability characteristics, the remote certificate requires the installation of drivers on desktop computers and the use of applications on mobile devices. These

complements will be provided to the user during the process of issuing the certificate and are therefore part of the service.

20. OTHER OBLIGATIONS OF THE APPLICANT/CERTIFICATE HOLDER

a) The CERTIFICATE HOLDER shall safeguard the remote signature activation key diligently and apply all appropriate measures to prevent damage to third parties as a result of the use of electronic signatures or authentication processes. The authentication tools for activating the remote signature procedure are strictly personal; the CERTIFICATE HOLDER is therefore required to protect the secrecy of such tools by not disclosing them to third parties in whole or in part and to store them securely.
b) CERTIFICATE HOLDERS must update their hardware and software systems to comply with the security requirements required by applicable laws.

Applies only to secure server certificates

SECTION III
TERMS AND CONDITIONS APPLICABLE TO
SECURE SERVER CERTIFICATES
(AUTHENTICATION OF WEBSITES/SSL, ELECTRONIC HEADQUARTERS)

21. OTHER OBLIGATIONS OF THE CA

If a third party directly detects or notifies any anomaly in the certificate issued, the CA shall notify this circumstance to the SUBSCRIBER within 24 hours and shall investigate and correct the problem within a period of five days. The CA may unilaterally revoke the certificate within the first 24 hours if it detects that the certificate has been incorrectly issued or if there is a serious security incident. If the certificate is revoked, CAMERFIRMA will substitute the certificate for a valid one as long as the anomaly could have been corrected, without the CERTIFICATE HOLDER/SUBSCRIBER claiming any compensation.

22. OTHER OBLIGATIONS OF THE APPLICANT/CERTIFICATE HOLDER

a) The APPLICANT must provide the CA or RA with an operational contact that enables the CA to notify the APPLICANT at any time of any incidents or anomalies related to the certificate, its revocation and replacement, if applicable.

b) The APPLICANT must collaborate and, if applicable, reliably provide the information and documentation required according to the type of web authentication certificate requested (OV-EV) necessary to prove the existence of the ENTITY/SUBSCRIBER and its ownership and control of the domain, all pursuant to the requirements that are determined at all times in the CABFORUM global community policies in its "Baseline Requirements" and "EV SSL Certificate guidelines", of which CAMERFIRMA is a member in its capacity as CA. By virtue of the foregoing, the ENTITY/SUBSCRIBER understands and expressly accepts that CAMERFIRMA's practices related to the web authentication service (and, therefore, the contractual conditions applied to the service), may be subject to variations and changes that affect the contracted certificate during its validity, without these changes being grounds for terminating the agreement or to compensation, provided they are due to being imposed by the CABFORUM community.

When AC CAMERFIRMA S.A. and the REGISTRATION AUTHORITY are in agreement with the previously stated ends, the APPLICANT shall read, on his or her own behalf, the entirety of this document and declare that he/she adheres completely to its content, which he/she formalises by accepting the agreement electronically, pursuant to current regulations regarding remote contracting.