GlobalSign Subscriber Agreement - Version 5.6

Notwithstanding the translation of this Agreement into a language other than English, the English language version of this Agreement shall at all times be controlling and the sole basis for interpretation of the terms herein.

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE CERTIFICATE ISSUED TO YOU OR YOUR ORGANIZATION. BY APPLYING FOR A CERTIFICATE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, CANCEL YOUR ORDER WITHIN SEVEN (7) DAYS OF THE AVAILABILITY OF THE CERTIFICATE FOR A FULL REFUND. IF YOU HAVE PROBLEMS UNDERSTANDING THIS AGREEMENT, E-MAIL US AT legal@globalsign.com

This GlobalSign Subscriber Agreement (the "Agreement") between GlobalSign and the Applicant or Subscriber (“You”) is effective as of the date of the application for the Certificate (the "Effective Date").

“GlobalSign” is the entity with which the Subscriber places an order to procure the Certificate, either GMO GlobalSign K.K. (Japan), GlobalSign China Co., Ltd. (China), GMO GlobalSign Ltd. (United Kingdom), GlobalSign NV (Belgium), GMO GlobalSign, Inc. (United States), GMO GlobalSign Pte. Ltd (Singapore), GMO GlobalSign Inc. (Philippines), GMO GlobalSign Certificate Services Pvt. Ltd (India), GMO GlobalSign Russia LLC (Russia), GMO GlobalSign Solutions in Technology S/A (Brazil) or GMO GlobalSign FZ LLC (United Arab Emirates). Notwithstanding the foregoing, if Subscriber orders an eIDAS Qualified Certificate “GlobalSign” shall mean GlobalSign NV (Belgium).

If you are a Procuring Party and are acting as the authorized representative of a Subscriber in applying for, or reselling a Certificate, you represent and warrant to GlobalSign and Relying Parties that you have obtained the authority of the Subscriber to enter into this Agreement on behalf of the Subscriber and that you shall comply with and procure Subscriber’s compliance with this Agreement.

If Subscriber procures the Certificate through a Procuring Party, then Subscriber hereby represents and warrants that Subscriber has authorized such Procuring Party to act on Subscriber’s behalf for the Certificate, including but not limited to the application, acceptance, operation, renewal and revocation of Subscriber’s Certificate. By authorizing a Procuring Party to provide or resell the Certificate to Subscriber, Subscriber hereby confirms its acceptance of this Agreement as it relates to Subscriber’s use of the Certificate. If Subscriber does not agree to the terms of this Agreement, then Subscriber may not purchase or use the Certificate of GlobalSign.

If the Subject and Subscriber are two separate entities and the Subject is a natural or legal person, Subscriber shall ensure that the Subject ratifies the requirements of this Agreement applicable to Subject.

1.0 Definitions and Incorporation by Reference

The following policies and associated guidelines are incorporated by reference into this Agreement:

- The GlobalSign Certification Practice Statement (CPS);
- The GlobalSign Warranty Policy; and
- The GlobalSign Payment Terms;

The current versions of the above GlobalSign documents are located at https://www.globalsign.com/en/repository/ and https://www.globalsign.com/en/company/corporate-policies.

The current versions of the CA/Browser Forum documents are located at https://cabforum.org/baseline-requirements-documents/.

The following definitions are used in this Agreement. Any terms used but not defined herein shall have the meaning ascribed to them in the Industry Standards.

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual Certificate request.

Application Software Supplier: A supplier of Internet browser software or other Relying Party application software that displays or uses Certificates and incorporates Root Certificates.

Authority Information Access: A Certificate extension that indicates how to access information and services for the issuer of the Certificate in which the extension appears.

CA/Browser Forum: An industry expert group of CA's and Application Software Suppliers. Details are available from www.cabforum.org.

Certificate: An electronic document that uses a Digital Signature to bind a Public Key and an identity. In the context of the MC Requirements, the certificate contains subject information and extensions specified in the MC Requirements and that has been verified and issued in accordance with these MC Requirements.

Certificate Beneficiaries: The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate, all Application Software Suppliers with whom GlobalSign has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier, and all Relying Parties who reasonably rely on a Valid Certificate.

Certificate Custodian: A nominated individual responsible for the lifecycle of the Certificate. This may or may not be the same entity as the Subscriber.

Certificate Requester: Applicant's representative who has express authority to represent the Applicant, or a third party (such as an ISP or hosting company) that completes and submits Certificate requests on behalf of the Applicant. Certificate Requesters can be pre-approved via the functionality of a GlobalSign managed service such as MSSL or EPKI.

Certificate Revocation List ("CRL"): A regularly updated timestamped list of revoked Certificates that is created and Digitally Signed by the CA that issued the Certificates.

Certification Authority ("CA"): An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs. In this document, the CA is GlobalSign or an entity which is certified by GlobalSign to issue the Certificate to the "Subject".

Digital Signature: To encode a message by using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's Public Key can accurately determine whether the transformation was created using the Private Key that corresponds to the signer's Public Key and whether the initial message has been altered since the transformation was made. Digitally Signed shall refer to electronic data to which a Digital Signature has been appended.

Domain Name: The label assigned to a node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

Domain Name System: An Internet service that translates Domain Names into IP addresses.

eIDAS Regulation ("eIDAS"): REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

Industry Standards: means the current versions of:

- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements")
- CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates ("EV Guidelines")
- CA/Browser Forum Network and Certificate System Security Requirements
- CA/Browser Forum Baseline Requirements for Code Signing ("Baseline Requirements for Code Signing")
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates ("Baseline Requirements for S/MIME")
- Minimum Security Requirements for Issuance of Mark Certificates ("MC Requirements")
- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers ("ETSI 319 401")

- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements ("ETSI 319 411-1")
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates ("ETSI 319 411-2")
- ETSI EN 319 421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps ("ETSI 319 421")
- ETSI TS 119 495: Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking ("ETSI 119 495")

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value.

Key Pair: The Private Key and its associated Public Key.

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

Mark Certificate: A Certificate that contains subject information and extensions specified in the MC Requirements and that has been verified and issued in accordance with the MC Requirements. GlobalSign only supports Verified Mark Certificates.

North American Energy Standards Board ("NAESB") Accreditation Requirements for Authorized Certification Authorities ("NAESB Accreditation Specification"): The technical and management details which a Certification Authority is required to meet in order to be accredited as an Authorized Certification Authority ("ACA") by NAESB.

Online Certificate Status Protocol ("OCSP"): An online Certificate-checking protocol that enables Relying Party application software to determine the status of an identified Certificate.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key. In the context of the MC Requirements, Once the Private Key-Public Key pair has been generated, the Private Key is not used and may be discarded. The Private Key is not used to create Digital Signatures and/or to decrypt records.

Procuring Party: A legal entity or business authorized by GlobalSign to resell or provide the Certificate to Subscriber.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key. In the context of the MC Requirements, the Public Key is not used to encrypt messages nor to verify Digital Signatures.

Qualified Certificate: A Certificate that meets the qualification requirements defined by the eIDAS Regulation.

Qualified Electronic Signature/Seal Creation Device (QSCD): An electronic signature/seal creation device that meets the requirements as stipulated within Annex II of eIDAS Regulation.

Registration Authority ("RA"): Any Legal Entity that is responsible for identification and authentication of Subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may

assist in the Certificate application process or revocation process or both. When “RA” is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Registered Mark: A type of mark included in a Mark Certificate that meets the requirements of section 3.2.17.1 of the MC Requirements.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such supplier merely displays information relating to a Certificate.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. If the Subject is a device or system, it must be under the control and operation of the Subscriber.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

Suspect Code: Code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user’s consent and/or resists its own removal or detection, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the platforms on which it executes.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with the GlobalSign CPS when the Applicant/Subscriber is an Affiliate of the CA.

Verified Mark Certificate: A certificate that contains subject information and extensions specified in the MC Requirements and that has been verified and issued in accordance with the MC Requirements. Additionally, the certificate contains a Mark Representation that has been verified as a Registered Mark.

Wildcard Certificate: A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

2.0 Authority to Use Certificates

2.1 Grant of Authority: From the Effective Date and for the term set forth within the validity period of any issued Certificate (“Valid from” date to “Valid to” date), GlobalSign hereby grants to the Subscriber the authority to use the Certificate in conjunction with Private Key and/or Public Key operations.

2.2 Limitations on Authority: The Subscriber shall use the Certificate only in connection with properly licensed cryptographic software.

3.0 Services Provided by GlobalSign

After acceptance of this Agreement and payment of applicable fees, in addition to the “Grant of Authority”, GlobalSign or a third-party provider designated by GlobalSign shall provide the following services from the time of issuance of the Certificate.

3.1 Provision of Certificate Revocation Lists (CRL), Online Certificate Status Protocol (OCSP) Services and Certificate Issuing Authority Details: GlobalSign shall use reasonable efforts to compile, aggregate and make electronically available for all Certificates signed and issued by GlobalSign's CA:

- CRLs for any Certificate containing a CRL Certificate distribution point;
- OCSP responders for any Certificates containing an OCSP responder URL, and
- Issuing Certificate information from the Authority Information Access locations; provided, however that GlobalSign shall not be in breach of its obligations hereunder as a result of any delay in or failure of performance on its part which arises out of any equipment failure or telecommunications breakdown beyond the reasonable control of GlobalSign.

3.2 Revocation Services for Certificates:
GlobalSign may revoke a certificate for the circumstances specified in the CPS or if GlobalSign receives notice or otherwise becomes aware that the Subscriber violated any of its material obligations under this Subscriber Agreement.

3.3 Key Generation: If Key Pairs are generated by GlobalSign on behalf of the Subscriber offered as Token or PKCS#12 options, GlobalSign will endeavor to use trustworthy systems in order to generate such Key Pairs, in which case, the following terms also apply.

- GlobalSign will generate Key Pairs using a platform recognized as being fit for such purpose and will ensure that Private Keys are encrypted if transported to the Subscriber,
- GlobalSign will use a key length and algorithm which is recognized as being fit for the purpose of Digital Signature, and
- In the case of both Code Signing and EV Code Signing Certificates, Subscriber acknowledges that GlobalSign will not sign Key Pairs that are smaller than 3072 bits.

GlobalSign does not generate Key Pairs for publicly trusted SSL certificates.

3.4 Site Seal Services for SSL/TLS Certificates and OCSP/CRL Responses: GlobalSign permits the Applicant to make use of GlobalSign's site seal on the Applicant's web site with a maximum daily rate of five hundred thousand (500,000) impressions per day. GlobalSign reserves the right to limit or stop the availability of the seal if this limit is exceeded.

GlobalSign provides a 24x7 service to check the validity of an issued Certificate either through an OCSP responder or CRL. A maximum daily rate of five hundred thousand (500,000) validations per Certificate per day is set. GlobalSign reserves the right to enforce OCSP stapling if this limit is exceeded.

3.5 Timestamping Services for Code Signing Certificate: GlobalSign offers the ability to timestamp code signed with a Code Signing Certificate as a non-chargeable service provided the service is used reasonably. As a best practice, GlobalSign recommends the Subscriber to timestamp the digital signature after signing his/her code, using the appropriate GlobalSign Timestamp Authority. GlobalSign establishes a limit of a reasonable number of timestamps for the validity period of the Code Signing Certificate and reserves the right to withdraw the service or charge additional fees for the service where the volume of timestamps is deemed excessive by GlobalSign.

3.6 Timestamping Services for Adobe Authorized Trust List (AATL) Certificate: GlobalSign may offer the ability to timestamp Portable Document Format (PDF) and Microsoft Office documents as a paid GlobalSign service. The number of signatures per year allowed by this service is established during the application process. GlobalSign reserves the right to withdraw the service or charge additional fees for the service where the volume of timestamps is in excess of the agreed limit.

4.0 Subscriber's Obligations and Warranties

Subscriber and/or Applicant warrants for the benefit of GlobalSign and the Certificate Beneficiaries that:

4.1 Accuracy of Information: Subscriber will provide accurate, complete and truthful information at all times to GlobalSign, both in the Certificate request and as otherwise requested by GlobalSign in connection with issuance of a Certificate, including but not limited to, the application name, information URL and application description in relation to Code Signing Certificates.

4.2 Protection of Private Key: Applicant (and if applicable, Subject) shall take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key to be associated with the requested Certificate(s) and any associated activation data or device, e.g. password or token.

For Code Signing Certificates, the Applicant must maintain sole control of, keep confidential, and properly protect, at all times in accordance with Section 4.15 below the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token). The Subscriber represents that it will generate and operate any device storing Private Keys in a secure manner, as described in a document of code signing best practices. The Subscriber must use passwords that are randomly generated with at least 16 characters containing uppercase letters, lowercase letters, numbers, and symbols to transport Private Keys.

4.3 Private Key Reuse: For Code Signing Certificates, the Applicant shall not apply for a Code Signing Certificate if the Public Key in the Certificate is or will be used with a non-Code Signing Certificate.

4.4 Prevention of Misuse: The Subscriber (and if applicable, Subject) will provide adequate network and other security controls to protect against unauthorized or misuse of the Private Key, and GlobalSign will revoke the Certificate without requiring prior notification if there is unauthorized access to the Private Keys.

4.5 Acceptance of Certificate: Subscriber shall not use the Certificates until after Applicant, or an agent of Applicant, has reviewed and verified the Certificate contents for accuracy. Unless the Subscriber notifies GlobalSign within seven (7) days from receipt, the Certificate is deemed accepted.

4.6 Use; Restrictions: Subscriber shall install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use.

Under no circumstances must the Certificate be used for criminal activities such as phishing attacks, fraud, certifying or signing malware. Subscriber should not use a Certificate to knowingly sign software that contains Suspect Code or otherwise distribute content that has the effect of misleading, inconveniencing or annoying the recipient such as software that includes unwelcome features or programs not disclosed appropriately to the user prior to installation, or is recognized as unwelcome or suspicious by commercial anti-virus scanning applications.

Subscriber shall use the Certificate and associated Private Key only for authorized and legal purposes, including not using the Certificate to sign Suspect Code and to use the Certificate and Private Key solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement.

4.6.1 PDF Signing: In the event a Certificate is used to sign a PDF, the Subscriber shall maintain information that permits a determination of who approved the signature of a particular document.

4.6.2 EV Code Signing: Subscriber accepts these additional obligations and makes the following warranties when using EV Code Signing Certificates:

- Only to sign code that complies with the requirements set forth in the latest version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates;
- Solely in compliance with all applicable laws;
- Solely for authorized company business; and
- Solely in accordance with this Agreement.

If Subscriber becomes aware (by whatever means) that it has signed code that contains malicious software or a serious vulnerability, the Subscriber must immediately inform GlobalSign.

4.6.3 Microsoft Stipulation: Subscriber acknowledges that Microsoft may independently determine that a Certificate is malicious or there has been a Key Compromise, and Microsoft services and applications may have the ability to modify Microsoft customer experiences to reflect Microsoft's determination without notice and without regard to the revocation status of the Certificate.

4.7 Reporting and Revocation:

Subscriber (and, if applicable, Subject):

- Agrees to cooperate with GlobalSign to comply with the applicable timelines and requirements for revocation, upon notification by GlobalSign or when becoming aware of a request for revocation;
- Acknowledges GlobalSign's obligations to adhere to Industry Standards, browsers' root programs requirements and other applicable policies and standards and accepts that the timeline for revocation may be days or hours depending on the circumstances; and
- Acknowledges, plans for and accepts responsibility for timely replacement of a Certificate.

GlobalSign encourages Subscribers to prepare and maintain actionable plans for replacing a Certificate affected by revocation.

Requests for revocation must be submitted through the account that requested Certificate or via report-abuse@globalsign.com.

4.7.1 Reasons for Revoking: Subscriber acknowledges having an understanding of the reasons for revoking a Certificate, including those stated in section 4.9.1 of the CPS.

Furthermore, Subscriber (and if applicable, Subject) shall promptly cease using a Certificate and its associated Private Key (except for key decipherment) and promptly request that GlobalSign revoke the Certificate if the Subscriber believes that (a) any information in the Certificate is, or becomes, incorrect or inaccurate, (b) the Private Key associated with the Public Key contained in the Certificate was misused, lost, stolen, potentially compromised, compromised, control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons, or (c) in the case of a Code Signing Certificate, there is evidence that the Certificate was used to sign Suspect Code.

4.7.2 Notifying GlobalSign of Status Changes: If a Certificate is issued to Subscriber ("New Certificate") on the basis of another valid Certificate held by the Subscriber ("Originating Certificate") and subsequently the Originating Certificate has been suspended or revoked, Subscriber is obligated to inform GlobalSign about the changed status of the Certificate. Upon such notice, GlobalSign will conduct investigations to determine whether it is necessary to suspend or revoke the New Certificate.

4.8 Termination of Use of Certificate: Subscriber (and if applicable, Subject) shall promptly cease use of the Private Key associated with the Public Key in the Certificate upon expiration or revocation of the Certificate or if the Issuing CA is compromised.

4.9 Responsiveness: Subscriber (and if applicable, Subject) shall respond to GlobalSign's instructions concerning Key Compromise or Certificate misuse within forty-eight (48) hours.

4.10 Acknowledgement and Acceptance: Subscriber has evaluated GlobalSign's CPS. Subscriber acknowledges and accepts that GlobalSign is entitled to revoke the Certificate immediately if the Applicant violates the terms of the Subscriber Agreement or if GlobalSign discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware. With respect to EV Code Signing Certificates used in connection with Microsoft services and applications, Subscriber further acknowledges that even though an EV Code Signing Certificate may not be revoked by

GlobalSign, Microsoft may independently determine that the Certificate is malicious or compromised and modify the Microsoft customer experience in the applicable Microsoft services and applications to reflect Microsoft's determination without notice and without regard to the revocation status of the Certificate.

4.11 Sharing of Information: With respect to Code Signing Certificates, Subscriber acknowledges and accepts that, if: (a) the Certificate or the Applicant is identified as a source of Suspect Code, (b) the authority to request the Certificate cannot be verified, or (c) the Certificate is revoked for reasons other than Subscriber request (e.g. as a result of Key Compromise, discovery of malware, etc.), then GlobalSign is authorized to share information about the Applicant, signed application, Certificate, and surrounding circumstances with other CAs or industry groups, including the CA/Browser Forum.

4.12 Compliance with Industry Standards: Subscriber acknowledges and accepts that GlobalSign may modify the Subscriber Agreement when necessary to comply with any changes in the Industry Standards, browsers' root programs requirements or any other applicable requirements.

4.13 Domain Control for SSL/TLS Certificate: The Subscriber acknowledges and asserts that s/he has control of the domain(s) or IP Address listed in the SubjectAltName(s) for which s/he is applying for the SSL/TLS Certificate. Should control cease for any domain(s), the Subscriber acknowledges that s/he must promptly inform GlobalSign in accordance with the obligations of the 'Reporting and Revocation' section.

4.14 Email Control for PersonalSign Certificate: The Subscriber acknowledges and asserts that s/he have control of the e-mail address for which they are applying for a PersonalSign Certificate. Should control cease for any e-mail address(s), the Subscriber acknowledges that s/he must promptly inform GlobalSign in accordance with the obligations of the 'Reporting and Revocation' section.

4.15 Key Generation and Usage: Where Key Pairs are generated by the Subscriber or the Certificate Requester, trustworthy systems must be used to generate Key Pairs, in which case, the following terms also apply:

- Key Pairs must be generated using a platform recognized as being fit for such purpose. In the case of AATL Certificates, this must be FIPS 140-2 Level 2 compliant,
- A key length and algorithm must be used which is recognized as being fit for the purpose of Digital Signature,
- The Subscriber shall ensure that the Public Key submitted to GlobalSign correctly corresponds to the Private Key used.

Where Key Pairs are generated in hardware (as required by the CPS):

- The Subscriber must maintain processes, including, without limitation, changing of activation data, that assure that each Private Key within a hardware security module (HSM) or token can be used only with the knowledge and explicit action of the "Certificate Custodian",
- The Subscriber must ensure that the Certificate Custodian has received security training appropriate for purposes for which the Certificate is issued, and
- Certificate Custodians undertake to take all reasonable measures necessary to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate, as well as any associated authentication mechanism to access the key (e.g., password to a token or HSM).

4.15.1 Code Signing and EV Code Signing:

For Non-EV Code Signing Certificates issued prior to April 24, 2023:

Subscriber represents that Subscriber will use one of the following methods to generate and protect their Code Signing Certificate Private Keys. GlobalSign recommends Subscribers use method 1 or 2 over method 3:

1. A Trusted Platform Module (TPM) that generates and secures a key pair and that can document the Subscriber's Private key protection through a TPM key attestation.
2. A hardware crypto module with a unit design form factor certified as conforming to at least FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent.
3. Another type of hardware storage token with a unit design form factor of SD Card or USB token (not necessarily certified as conformant with FIPS 140 Level 2 or Common Criteria EAL 4+). Subscriber also warrants that it will keep the token physically separate from the device that hosts the code signing function until a signing session is begun.

For EV Code Signing Certificates issued prior to April 24, 2023:

The Subscriber's private key must be generated, stored and used in a crypto module that meets or exceeds the requirements of FIPS 140-2 level 2 or Common Criteria EAL 4+.

Effective April 24, 2023, for Non-EV and EV Code Signing Certificates:

Subscriber represents that Subscriber will use one of the following options to generate and protect their Code Signing Certificate Private Keys in a Hardware Crypto Module with a unit design form factor certified as conforming to at least FIPS 140-2 Level 2 or Common Criteria EAL 4+:

- Subscriber uses a Hardware Crypto Module meeting the specified requirement.
- Subscriber uses a cloud-based key generation and protection solution with the following requirements: a. Key creation, storage, and usage of Private Key must remain within the security boundaries of the cloud solution's Hardware Crypto Module that conforms to the specified requirements; b. Subscription at the level that manages the Private Key must be configured to log all access, operations, and configuration changes on the resources securing the Private Key.
- Subscriber uses a Signing Service which meets the requirements of Section 6.2.7.3 of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates".

At any time during the application and life cycle of the Certificate, Subscriber must be able to, on request of GlobalSign, present proof that Key Pair is generated and protected in accordance with these requirements. Failure to provide such evidence might result in revocation of the Certificate.

4.15.3 Qualified: For Qualified Certificates, Subscriber (and if applicable, Subject) acknowledges and accepts that:

- Private Keys must be maintained (or respectively used) under the Subject's sole control (in case of Qualified Certificates for electronic signatures) or Subject's control (in case of Qualified Certificates for electronic seals),
- Private Keys shall only be used for electronic signatures (in case of Qualified Certificates for electronic signatures) or electronic seals (in case of Qualified Certificates for electronic seals),
- If the holder of the Qualified Certificate for electronic seals is established in Belgium, the holder shall take measures to be able to establish the name, capacity and power of attorney of the natural person representing the legal person, who makes practical use of the Certificate, in such a way that each time that Certificate is used, the holder and, where appropriate, the competent administrative or judicial authorities acting in the context of detecting and establishing infringements can establish the identity and representation rights of the natural person.

For Qualified Certificates that require a Qualified Signature or Seal creation device (QSCD):

- Digital signatures shall only be created by a QSCD device,
- Private Keys must be generated and stored within a certified QSCD, which has either been supplied or approved in writing by GlobalSign,

- The QSCD certification status must be monitored by the Subscriber and appropriate measures must be taken if the certification status of the QSCD changes.

4.16 NAESB Certificates

Subscribers for NAESB Certificates acknowledge their understanding of the following obligations of the NAESB Wholesale Electric Quadrant Business Practice Standards WEQ-012 (the "WEQ PKI Standards"): Subscribers participating in the WEQ PKI Standards shall be required to be registered in the NAESB EIR and furnish proof that they are an entity authorized to engage in the wholesale electricity industry. Entities or organizations that may require access to applications using authentication specified under the WEQ PKI Standards, but do not qualify as a wholesale electricity market participant (e.g., regulatory agencies, universities, consulting firms, etc.) must register.

Registered end entities and the user community they represent shall be required to meet to all end entity obligations in the WEQ PKI Standards.

Subscriber organization certifies to GlobalSign that it has reviewed and acknowledges the following WEQ PKI Standards:

4.16.1. Subscriber acknowledges the electric industry's need for secure private electronic communications that facilitate the following purposes:

- Privacy: The assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended;
- Authentication: The assurance to one entity that another entity is who he/she/it claims to be;
- Integrity: The assurance to an entity that data has not been altered (intentionally or unintentionally) between "there" and "here," or between "then" and "now"; and
- Non-Repudiation: A party cannot deny having engaged in the transaction or having sent the electronic message.

4.16.2 Subscriber acknowledges the industry's endorsement of Public Key cryptography which utilizes Certificates to bind a person's or computer system's Public Key to its entity and to support symmetric encryption key exchange.

4.16.3 Subscriber has reviewed the WEQ PKI Standards with respect to industry guidelines for establishing a trusted PKI.

4.16.4 Subscriber has evaluated GlobalSign's CPS in light of those industry standards.
If applicable, Subscribers shall be obligated to register their legal business identification and secure an "Entity Code" that will be published in the NAESB EIR and used in all Subscriber applications submitted by, and Certificates issued to, that end entity. In complying with the WEQ-012 requirements, when issuing Certificates for use within the energy industry for other than WEQ-012 applications, ACAs must comply with the provisions of the WEQ PKI Standards, except provisions in WEQ-012.12.1.9, WEQ-012-1.3.3, and WEQ-012.1.4.3, which require end entity registration within the NAESB EIR.

Subscribers shall also be required to comply with the following requirements:

- Protect their Private Keys from access by other parties.
- If applicable, identify, through the NAESB EIR, that they have selected GlobalSign to use as their ACA.
- Execute all agreements and contracts with GlobalSign necessary for GlobalSign to issue Certificates to the end entity for use in securing electronic communications.
- Comply with all obligations required and stipulated by GlobalSign in its CPS, e.g., Certificate application procedures, Applicant identity proofing/verification, and Certificate management practices.

- Confirm that it has a Certificate management program, has trained all affected employees in that program, and has established controls to ensure compliance with that program. This program shall include, but is not limited to:
- Certificate Private Key security and handling policy(ies)
- Certificate revocation policy(ies)
- Identify the type of Subscriber (I.e., individual, role, device or application) and provide complete and accurate information for each Certificate request.

4.17 Mark Certificates

Subscribers for Mark Certificates further agree to the following terms of use ("MC Terms"):

All Mark Asserting Entities (MAEs) are required, as a condition of being issued a Mark Certificate, to agree to these MC Terms. Any and all use, display, or reliance on any Mark Certificate (and any Mark Representation and any other data or information therein) by Consuming Entities, Relying Parties, and any other person, is subject to and conditional upon acceptance of these MC Terms. The OID 1.3.6.1.4.1.53087.1.1 in the Mark Certificate incorporates by reference these MC Terms. If any person does not agree to these MC Terms, such person may not obtain, use, publish, or rely upon any Mark Certificate or on any Mark Representation or any other data or information in a Mark Certificate.

4.17.1. Definitions.
Capitalized words will have meanings set out in Section 1.6 of the MC Requirements.

4.17.2. Limited Right to Reproduce and Display.
The MAE hereby grants, subject to the terms, conditions and restrictions in the MC Requirements and these MC Terms:

4.17.2.1. to the Issuing CA, a limited, non-exclusive, worldwide license to issue a Mark Certificate that contains the MC Marks and to log said Certificate in a limited number of Certificate Transparency Logs as required by the MC Requirements; and

4.17.2.2. to Consuming Entities, a limited, non-exclusive, worldwide license to use the MC Marks in conjunction with internal logo recognition systems, and to host, store, reproduce, display, process, and modify as permitted by section 4.17.3.1, the MC Marks only in direct visual association with communications, correspondence, or services authored or provided by the MAE from or through one of the same domains included within the Mark Certificate's Subject Alternative Name field; and

4.17.2.3. to certificate transparency log operators (if different from the Issuing CA), a limited, nonexclusive, worldwide license to retain a copy of and to reproduce the Mark Certificate to support a durable public record of those issued Certificates, and for the purpose of permitting members of the public to audit the verification of Mark Certificates. No other license is granted to any other party, or for any other use.

4.17.3. License Restrictions and Conditions.
Any Consuming Entity that incorporates or intends to incorporate the MC Marks obtained through an issued and published Mark Certificate into its products and services, agrees that its license to do so is subject to and conditional on the following:

4.17.3.1. Quality Control, Same Treatment.
The Consuming Entity may not distort at display time any Mark Representation obtained from a published Mark Certificate, change its colors or background, modify its transparency, or alter it in any way other than to adjust its size or scale, or to crop it in a manner consistent with cropping performed on other Mark Representations displayed in the same context. If a Consuming Entity displays a Word Mark obtained from a published Mark Certificate, it must do so in a neutral manner applied consistently to all Word Marks from all Mark Certificates that are shown in the same visual context. The Consuming Entity may display a Mark included in a Mark Certificate without also displaying a

Word Mark included in the same Mark Certificate, but the Consuming Entity may not display a Word Mark included in a Mark Certificate without also
displaying the Mark included in the same Mark Certificate.

4.17.3.2. No Partnership or Relationships implied.
Subject to an express agreement to the contrary between the Consuming Entity and the MAE, neither the MC Marks nor any other content of the Mark Certificate may be used or displayed in any way that reasonably implies any relationship between the Consuming Entity and the MAE, beyond the bare licensor-licensee relationship created by these MC Terms.

4.17.3.3. CRL or OCSP Checks.
Consuming Entities must check the Certificate Revocation Lists maintained by the CA or perform an on-line revocation status check using OCSP to determine whether a Mark Certificate has been revoked no less frequently than every 7 days.

4.17.3.4. Lawful Use
Consuming Entities may only use the Mark Representation in a Mark Certificate in accordance with applicable law.

4.17.3.5. Sufficient Ownership or License.
The MAE warrants that the MC Marks published via a Mark Certificate represent a Registered Mark (and Word Mark, if any) that the MAE owns or for which the MAE has obtained sufficient license to be able to grant the limited license in these MC Terms, and that it will immediately revoke the Mark Certificate if it no longer owns or has a sufficient license to the applicable Registered Mark (or Word Mark, if any). The MAE will defend and will be liable for any intellectual property or other claims against any Consuming Entity, Relying Party or CA that arise from the content of the MAE's application for a Mark Certificate.

4.17.3.6. No Obligation to Display.
The MAE acknowledges that Consuming Entities are under no obligation to display the MC Marks in connection with content the MAE publishes that is associated with the domains the MAE owns or controls as a Domain Registrant, even if a communication or message is confirmed to be from the MAE and a suitable MC Mark can be obtained and safely displayed from the applicable Mark Certificate. Instead, Consuming Entities may choose to display the MC Marks in accordance with these MC Terms, or not display them, at their option.

4.17.3.7. Termination.
Immediately upon revocation or expiration of the Mark Certificate, the MAE will cease publishing or using the Mark Certificate, and the license granted to Consuming Entities in Section 4.17.2 above shall terminate. The license to a Consuming Entity in Section 4.17.2 above also terminates automatically and immediately upon breach of any provision of these MC Terms by the Consuming Entity. Consuming Entities must immediately cease any and all use of the MC Marks upon termination of the applicable license.

4.17.3.8. Updates to MC Requirements and MC Terms.
The MC Requirements and MC Terms may be updated from time to time. All parties agree that the version of the MC Requirements and MC Terms in effect at the time of issuance of a Mark Certificate shall apply through the date of expiration or revocation of the Mark Certificate (and, for those provisions that by their nature extend beyond the date of expiration or revocation, until the provisions no longer would apply by their terms). It is the responsibility of each entity who obtains, uses, publishes or relies upon a Mark Certificate to review and familiarize itself from time to time with any updated versions of the MC Requirements and MC Terms.

5.0 Credentials

GlobalSign may provide credentials to access and/or use Services or Certificates. You are responsible for maintaining the confidentiality and security of your credentials and are fully responsible for all activities that occur with these credentials.

6.0 Fees

If the Certificate was purchased through a GlobalSign Procuring Party, Subscriber shall pay the Procuring Party according to the payment terms agreed between Subscriber and the Procuring Party.

Subscriber acknowledges and agrees that (i) if Subscriber does not pay the applicable fees (for example where Subscriber has procured the Certificate through a Procuring Party and Subscriber does not pay the applicable fees to the Procuring Party), or (ii) if the Procuring Party does not pay GlobalSign the applicable fees in accordance with GlobalSign's agreement with Procuring Party, regardless if the Subscriber pays the applicable fees to the Procuring Party, then Subscriber may not use the Certificate and GlobalSign may revoke the issued Certificates for which fees are outstanding.

7.0 Consent to Publish Information

By providing personal information when applying for a Certificate, Subscriber consents to GlobalSign's disclosure of this information publicly by (i) embedding the information issued in the Certificate and (ii) publishing the Certificate in Certificate Transparency (CT) logs.

8.0 Test Certificates

GlobalSign may provide or support issuing Certificates for testing and evaluation purposes, including but not limited to trial evaluation, interoperability testing and proof-of-concepts ("Test Certificate(s)"). Subscriber may only use a Test Certificate in an internal, non-production environment and as part of non-commercial evaluation.

The right to use a Test Certificate may be limited in time and further restricted in additional agreements between Subscriber and GlobalSign, in which case Subscriber's right to use will be terminated after the end date specified. GlobalSign may at its sole discretion terminate the right of use of any Test Certificate at any time. Subscriber shall cease the use of the Test Certificate upon such termination.

Warranty Disclaimer. SUBSCRIBER ACKNOWLEDGES THAT TEST CERTIFICATES ARE PROVIDED "AS IS" AND WITHOUT ANY WARRANTY WHATSOEVER. TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW, GLOBALSIGN EXPRESSLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT, RELATING TO ANY TEST CERTIFICATES, SUBSCRIBER'S USE OR ANY INABILITY TO USE A TEST CERTIFICATES, THE RESULTS OF ITS USE AND THIS AGREEMENT.

LIMITATION OF LIABILITY. GLOBALSIGN SHALL NOT BE LIABLE TO SUBSCRIBER FOR ANY CLAIMS, DEMANDS OR DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DIRECT, INDIRECT, CONSEQUENTIAL OR SPECIAL DAMAGES, ARISING OUT OF THE USE OF ANY TEST CERTIFICATES AND THE USE OR FAILURE OF A TEST CERTIFICATE TO OPERATE FOR WHATEVER REASON, WHETHER SUCH ACTION IS BASED IN CONTRACT OR TORT OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, NEGLIGENCE.

9.0 GlobalSign Limited Warranty

EXCEPT TO THE EXTENT PROHIBITED BY LAW OR AS OTHERWISE PROVIDED HEREIN, GLOBALSIGN DISCLAIMS ALL WARRANTIES INCLUDING ANY WARRANTY OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE.

TO THE EXTENT GLOBALSIGN HAS ISSUED AND MANAGED THE CERTIFICATE IN ACCORDANCE WITH THE CPS, GLOBALSIGN SHALL NOT BE LIABLE TO THE SUBSCRIBER, RELYING PARTY OR ANY THIRD PARTIES FOR ANY LOSSES SUFFERED AS A RESULT OF USE OR RELIANCE ON SUCH CERTIFICATE. OTHERWISE, GLOBALSIGN'S LIABILITY TO THE SUBSCRIBER, RELYING PARTY OR ANY THIRD PARTIES FOR ANY SUCH LOSSES SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS ($1,000) PER SUBSCRIBER OR RELYING PARTY PER CERTIFICATE; PROVIDED HOWEVER THAT THE LIMITATION SHALL BE TWO THOUSAND DOLLARS ($2,000) PER SUBSCRIBER OR RELYING PARTY PER CERTIFICATE FOR AN EV, EV CODE SIGNING OR MARK CERTIFICATE.
THIS LIABILITY CAP LIMITS DAMAGES RECOVERABLE OUTSIDE OF THE CONTEXT OF THE GLOBALSIGN WARRANTY POLICY. AMOUNTS PAID UNDER THE WARRANTY POLICY ARE SUBJECT TO THEIR OWN LIABILITY CAPS.

IN NO EVENT SHALL GLOBALSIGN SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES, OR FOR ANY LOSS OF PROFITS, LOSS OF DATA OR OTHER INDIRECT, INCIDENTAL, CONSEQUENTIAL DAMAGES ARISING FROM OR IN CONNECTION WITH THE USE, DELIVERY, RELIANCE UPON, LICENSE, PERFORMANCE OR NON PERFORMANCE OF CERTIFICATES, DIGITAL SIGNATURES OR ANY OTHER TRANSACTIONS OR SERVICES OFFERED OR CONTEMPLATED BY THIS SUBSCRIBER AGREEMENT.

THIS LIABILITY LIMITATION SHALL BE THE SAME REGARDLESS OF THE NUMBER OF DIGITAL SIGNATURES, TRANSACTIONS, OR CLAIMS RELATED TO SUCH CERTIFICATE.

THE FOREGOING SHALL NOT LIMIT GLOBALSIGN'S LIABILITY WITH RESPECT TO QUALIFIED CERTIFCATES IN ACCORDANCE WITH ARTICLE 13 OF THE EIDAS REGULATION.

10.0 Term and Termination

This Agreement shall terminate upon the earliest of:

- The expiration date of the Certificate issued to the Subscriber either directly, indirectly or through a MSSL or ePKI service that has not yet expired; or
- Failure by the Subscriber to perform any of its material obligations under this Agreement if such breach is not cured within five (5) days after receipt of notice thereof from GlobalSign.

11.0 Effect of Termination

Upon termination of this Agreement for any reason, GlobalSign may revoke the Subscriber's Certificate in accordance with GlobalSign procedures. Upon revocation of the Subscriber's Certificate, all authority granted to the Subscriber pursuant to Section 2 shall terminate. Such termination shall not affect Sections 4, 5, 6, 7, 8 and 11 of this Agreement, which shall continue in full force and effect to the extent necessary to permit the complete fulfillment thereof.

12.0 Miscellaneous Provisions

12.1 Governing Law and Venue

The (i) laws that govern the interpretation, construction, and enforcement of this Agreement and all matters, claims or disputes related to it, including tort claims, and (ii) the courts that have exclusive jurisdiction over any of the matters, claims or disputes, are set forth in the table below.

GlobalSign Entity on Order Summary	Governing Law	Venue
GMO GlobalSign K.K.	Japan	Tokyo District Court, Japan
GlobalSign China Co., Ltd.	China	Shanghai, China
GMO GlobalSign Ltd.	England and Wales	London, England
GlobalSign NV	Belgium	Leuven, Belgium
GMO GlobalSign, Inc. (US)	New Hampshire, USA	State and federal courts of New Hampshire
GMO GlobalSign Pte. Ltd	Singapore	Singapore
GMO GlobalSign Inc.	Philippines	Makati City, Philippines
GMO GlobalSign Certificate Services Pvt. Ltd	Laws of Republic of India	Delhi, India
GMO GlobalSign Russia LLC	Russia Federation Laws	Moscow, Russia
GMO GlobalSign Solutions in Technology S/A	Brazil	Belo Horizonte, Brazil
GMO GlobalSign FZ LLC	United Arab Emirates	Dubai, United Arab Emirates

For eIDAS Qualified Certificates, disputes related to financial or commercial matters will be handled in accordance with the governing law and venue shown above, and for certificate related disputes, the governing law and venue for will be as shown above for GlobalSign NV.

12.2 Binding Effect

Except as otherwise provided herein, this Agreement shall be binding upon, and inure to the benefit of, the successors, executors, heirs, representatives, administrators and assigns of the parties hereto. Neither this Agreement not the Subscriber's rights in the Certificate shall be assignable by the Subscriber. Any such purported assignment or delegation shall be void and of no effect and shall permit GlobalSign to terminate this Agreement.

12.3 Entire Agreement

This Agreement, along with all documents referenced herein, any product or service agreement, and the reseller agreement (if you are a reseller) constitute the entire agreement between the parties and supersedes any prior oral or written agreements, commitments, understandings, or communications with respect to the subject matter of this Agreement.

12.4 Severability

If any provision of this Agreement, or the application thereof, shall for any reason and to any extent, be invalid or unenforceable, the remainder of this Agreement and application of such provision to other persons or circumstances shall be interpreted so as best to reasonably effect the intent of the parties hereto. IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT EACH AND EVERY PROVISION OF THIS AGREEMENT WHICH PROVIDES FOR A LIMITATION OF LIABILITY, DISCLAIMER OF WARRANTIES OR EXCLUSION OF DAMAGES IS INTENDED BY THE PARTIES TO BE SEVERABLE AND INDEPENDENT OF ANY OTHER PROVISION AND TO BE ENFORCED AS SUCH.

12.5 Notices

Whenever Subscriber desires or is required to give any notice, demand, or request to GlobalSign with respect to this Agreement, each such communication shall be in writing and shall be effective only if it is delivered by a courier service that confirms delivery in writing or mailed, certified or registered mail, postage prepaid, return receipt requested, addressed to GlobalSign at one of our International offices as listed at https://www.globalsign.com/en/company/contact, Attention: Legal Department. Such communications shall be effective when they are received.

12.6 Compliance with export laws

Each party will comply with all applicable federal, state, and local laws and regulations in connection with its performance under this Agreement, including but not limited to, all applicable sanction laws, import and export laws, restrictions, national security controls, and regulations (collectively “Laws”). Subscriber will not import, export, re-export, or authorize the export or re-export of any Certificate or any other product in violation of any Laws.

12.7 Privacy; Use of third-party databases

GlobalSign shall follow its privacy policy on its website (which can be found at https://www.globalsign.com/en/repository) when receiving and using information from Subscriber. GlobalSign may amend the privacy policy at any time by posting the amended privacy policy on its website.

After Subscriber provides personal information to GlobalSign when applying for a Certificate, GlobalSign may process, disclose and/or transfer this information on a global basis to its affiliates, agents and subcontractors as necessary to validate and issue a Certificate, including processing, disclosure and/or transfer to countries that may have data protection laws that are less protective than those in the country where Subscriber is located.

For natural persons, GlobalSign may validate items such as name, address and other personal information supplied during the application process against appropriate third party databases. This is necessary in order for GlobalSign to provide the services and in performing these checks, personal information provided by the Subscriber may be disclosed to registered credit reference agencies, which may keep a record of that information. Such check is done only to confirm identity, and as such, a credit check is not performed. The Subscriber’s credit rating will not be affected by this process.

If you placed your order with GMO GlobalSign Russia LLC, GlobalSign may, for natural persons, validate items such as name, address and other personal information supplied during the application. This is

necessary in order for GlobalSign to provide the services and GlobalSign may process Subscriber's personal data in any of the following ways: collecting, classifying, processing, storing, editing, using, depersonalizing, blocking and deleting, as stated by Russian Federal Law FZ-No.152 at 27.07.2006, as well as transferring to third parties in cases established by regulations of the higher authorities and the law.

If you placed your order with GMO GlobalSign Philippines (GSPH), GlobalSign may, for natural persons, validate items such as name, address and other personal information supplied during the application. This is necessary in order for GlobalSign to provide the services and GlobalSign may process Subscriber's personal data in any of the following ways: collecting, classifying, processing, storing, editing, using, depersonalizing, blocking and deleting, as stated by Republic Act 10173 or the Philippine Data Privacy Act of the 2012, as well as transferring to third parties in cases established by regulations of the higher authorities and the law.

12.8 Trade Names, Logos

By reason of this Agreement or the performance hereof, Subscriber and GlobalSign shall acquire no rights of any kind in any trademark, brand name, logo or product designation of the other party and shall not make any use of the same for any reason except as otherwise authorized in writing by the party which owns all rights to such trademarks, trade names, logos or product designation.

13.0 Customer Support

For support queries, Subscribers can contact GlobalSign via support@globalsign.com or through any of our international offices listed or on https://www.globalsign.com/en/company/contact.

13.1 Refund Policy

If Subscriber is not completely satisfied with the issued Certificate, if the Certificate was ordered directly from GlobalSign, Subscriber may request a refund within seven (7) days of the Certificate being issued. Any refunds will be net of any fees incurred by GlobalSign.

[V 5.6 August 28, 2025]