

TERMS AND CONDITIONS FOR GLOBAL TRUSTED SIGN CERTIFICATES

Global Trusted Sign

Document Reference | FO23_GTS_V16

Table of Contents

1 TERMS AND CONDITIONS FOR THE USE OF QUALIFIED AND/OR ADVANCED-CERTIFICATES ISSUED BY GLOBAL TRUSTED SIGN.....	3
2 QUALIFIED AND/OR ADVANCED TRUST SERVICES.....	3
3 DATA PROTECTION AND STORAGE.....	5
4 USE RESTRICTIONS	10
5 SUBSCRIBER RIGHTS	11
6 SUBSCRIBER OBLIGATIONS	12
6.1 CERTIFICATE ISSUANCE PROCESS AND HOLDER IDENTITY VALIDATION	13
6.2 REISSUANCE OF CERTIFICATES.....	15
6.3 DCs REVOCATION.....	16
6.4 AMENDMENTS TO THE CERTIFICATE ISSUANCE FORM	16
7 GLOBAL TRUSTED SIGN OBLIGATIONS.....	16
8 OBLIGATIONS LIMITS.....	16
9 USE OF THE SERVICE.....	17
10 PRICE AND PAYMENTS.....	17
11 SHARING INFORMATION WITH THIRD PARTIES	18
12 PRESERVATION OF AUDIT LOGS	18
13 AVAILABILITY OF SERVICES.....	19
14 COMPENSATIONS.....	19
15 CONTACTS.....	19
16 RIGHT OF WITHDRAWAL.....	20
17 EFFECTS OF WITHDRAWAL	20
18 CONTACT OF THE DATA PROTECTION OFFICER	21
19 DISPUTE SETTLEMENT PROVISIONS	21
20 APPLICABLE LEGISLATION	21

1 TERMS AND CONDITIONS FOR THE USE OF QUALIFIED AND/OR ADVANCED-CERTIFICATES ISSUED BY GLOBAL TRUSTED SIGN

A Global Trusted Sign provides a set of online services that allows the acquisition of digital products as a qualified trust service provider.

The use of the services is subject to the following terms of use, with this document constituting an agreement between the subscriber/certificate holder and Global Trusted Sign.

The acquisition of certificates requires prior registration on the platform www.globaltrustedsign.com, with the creation of a username and password, which are strictly personal and non-transferable.

2 QUALIFIED AND/OR ADVANCED TRUST SERVICES

These terms and conditions apply to the use of digital certificates issued by Global Trusted Sign, including qualified certificates (signatures, seals, and SSL/TLS certificates) and advanced certificates (signatures and seals).

The subscriber/certificate holder must carefully read each document before acquiring any certificate provided by Global Trusted Sign services.

Any change to the email address used by the subscriber/certificate holder to access the platform/certificates must be communicated to Global Trusted Sign whenever it affects access to the platform or the receipt of notifications. If the subscriber/certificate holder loses access to the account, they must request the revocation of the associated certificates and proceed to acquire new ones.

Advanced Certificates

- Advanced digital certificates offer a high level of trust; however, they do not guarantee the evidentiary value of qualified certificates.
- The decision to read and electronically sign a document does not affect the legal consequences that such an action may entail.

Qualified Certificates

- Qualified Electronic Signatures and Seals

- A qualified electronic signature and a qualified electronic seal are legally equivalent to a handwritten signature.
- They carry evidentiary value in the European Union and in other countries that recognize Regulation (EU) No. 2024/1183.

- The user acknowledges that:
 - Qualified certificates are legally binding in Europe and several other countries;
 - Printed copies of documents with qualified signatures do not have the same legal value as the original electronic versions;
 - Global Trusted Sign and relying parties must be notified whenever the user changes their email address;
 - In the case of professional certificates, Global Trusted Sign must be notified if the user ceases to perform the professional roles indicated in the certificate;
 - The decision to read and sign a document does not change the legal effects of the qualified signature.

- SSL/TLS Certificates

Qualified **SSL/TLS** certificates are used to:

- Establish **secure web-based communication through** SSL/TLS protocols;
- Comply with **Regulation (EU) No. 2024/1183**.

Primary purposes:

- **Identify the legal entity** that controls a website:
 - Ensures the user that the website is controlled by an **identifiable entity**, with data such as company name, registered address, and legal registration.
- **Enable encrypted communications with the website:**
 - Facilitate **key exchange** to ensure the **confidentiality of information exchanged** between the browser and the website.
- **Extended Validation Certificates (EV SSL)**
- EV certificates offer a more rigorous identity verification process.

Benefits of EV SSL:

- Make **phishing attacks** and identity fraud using certificates **more difficult**;
- **Support companies that are victims** of fraud by providing a way to identify themselves to users;
- **Assist legal investigations** by facilitating contact with the certificate holder and legal action when applicable.
- **Trust and Compliance Assurance:**
 - Relying parties can **verify the trust chain** of certificates issued by Global Trusted Sign, ensuring the **authenticity and identity of the certificate holder**.

- SSL certificates **protect the security and confidentiality** of user-submitted data, in accordance with **Article 32, nº1, b) of the General Data Protection Regulation (GDPR)**.

3 DATA PROTECTION AND STORAGE

Qualified Certificates for Electronic Signatures

- May be issued in the following formats:
 - **Individual:** for a natural person or under a pseudonym;
 - **Organizational:** on behalf of a legal entity.
 - **Professional individual:** for a natural person with defined professional attributes.
 - **Professional collective:** for a legal entity with specified professional roles or functions.
 - **Seal:** legal entity.

Advanced Certificates

- May be issued in the following formats:
 - **Individual:** for a natural person or under a pseudonym;
 - **Organizational:** on behalf of a legal entity;
 - **Professional Individual:** for a natural person with defined professional attributes;
 - **Professional Organizational:** for a legal entity with specified roles or professional functions.
 - **Seal:** collective entity.

Global Trusted Sign ensures that the data collected through the forms for advanced certificates are processed in accordance with the General Data Protection Regulation (GDPR). This data includes name, email, professional contacts, and any identity documents associated with the issuance of the certificate.

The data is securely stored and used exclusively for purposes related to the issuance, management, reissuance, or revocation of the certificates.

Global Trusted Sign undertakes to obtain the explicit consent of the data subject before initiating any non-essential processing or for external communication purposes.

Global Trusted Sign also informs that, for the issuance of any certificate, the holder must first register on the Global Trusted Sign platform by creating a username and password, thereby ensuring the authenticity and traceability of the identification process.

SSL/TLS Certificates

- May be issued in the following formats:
 - **Individual;**
 - **Organizational.**

Data Collection and Protection of Personal Information

- To obtain any type of certificate, users must complete the corresponding **issuance form**, in which **personal and sensitive data is requested**.
- In accordance with the **General Data Protection Regulation (GDPR)**, data stored on remote servers must comply with strict **protection requirements, in order to:**
 - **Safeguard the privacy** of data subjects;
 - **Ensure the security of the information** collected and stored.

Global Trusted Sign declares that all requested and collected data is necessary to ensure secure means of electronic identification, and to prevent the misuse of the certificate holders' identities.

Time limits for the storage of information	
Information requested during the registration	At the time of registration, information regarding the name, surname, phone contact, email, TIN, country and desired password, is requested. This information is stored during 180 consecutive days from the registration date. After that period, and if the customer does not express interest to buy any of Global Trusted Sign available products, that information will be deleted.
From the selection of the service to the due payment	The information of the individual or legal entity required for the acquisition of services will be retained for a period of 180 consecutive days , counted from the date of registration or completion of the issuance form , as applicable.

Time limits for the storage of information	
	• If the product issuance form is completed but payment is not made, all collected information will be automatically deleted after 180 days. • If the user only selects the product without completing the corresponding form, and only billing information is provided (which may include personal or company data), such data will be processed exclusively for administrative and accounting purposes, in accordance with Global Trusted Sign's Privacy Policy, and retained for the legally required periods. • If the user wishes to rejoin the platform and acquire a new service after the aforementioned period, a new registration must be completed and, if applicable, the issuance form must be filled out again.
From form completion to identity verification	In the case of Qualified Certificates for Electronic Signatures (for either legal entities or individuals) and Qualified Certificates for Electronic Seals, once the issuance form has been completed, the terms and conditions have been duly signed and submitted, and, where applicable, payment has been made, the certificate holder will receive a notification to schedule identity verification. Identity verification may be carried out by: • Videoconference, in accordance with GNS Order No. 154/2017; • In person; • Or through authentication using a Citizen Card.

Time limits for the storage of information	
	If the certificate holder (or representative, in the case of a legal entity) does not complete the identity verification within 180 days from the date of form submission, a notification will be issued to reschedule the verification within the following 7 days. If verification is not completed within these deadlines, all collected data will be deleted. In the case of advanced certificates, a video conference or another identity verification method will only be carried out if there are doubts about the applicant's identity.
From the identity validation to the issuance of the certificate	Once the identity (of the legal entity or natural person) has been confirmed, the holder must issue/generate the certificate within a maximum period of 180 consecutive days. If this period is exceeded, the holder will be notified to proceed with the issuance of the certificate within the following 15 days. After this period, their data will be deleted. If it is necessary to repeat the video conference due to the failure to generate the certificate within the required period, a new appointment will be necessary, subject to an additional fee of 10 euros (+VAT at the applicable rate). In the case of advanced certificates, the generation of the certificate is the responsibility of the trust service provider and will subsequently be associated with the certificate profile after validation of the request data.
Period of inactivity	In the case of qualified certificates for electronic signatures, qualified certificates for electronic seals, and certificates for website authentication, if an account remains inactive for a period of 9 months, the legal entity/natural person/user will be notified and

Time limits for the storage of information	
	informed that they have 270 days to log in. If the aforementioned period is exceeded, the holder will be notified to access the platform and log in within the following 30 days. Otherwise, the account will be deleted. With regard to advanced electronic seal certificates and advanced electronic signature certificates, if Global Trusted Sign detects that an account has been inactive for a period of 9 months, the legal entity/natural person/user will be notified and informed that they have 30 days to log in. Otherwise, the account will be deleted. In the case of advanced certificates, account inactivity does not limit the use of the certificate, as it is used locally after being downloaded.
Time limit for the right to data portability	When the right to data portability is exercised by a legal entity, individual, subscriber, or user, Global Trusted Sign will carry out the corresponding action within a maximum period of 60 days. The right to data portability applies exclusively to personal data provided by the data subject, where the processing is based on consent or the performance of a contract, and is carried out by automated means. Whenever these conditions are not met, Global Trusted Sign reserves the right to refuse the portability request, informing the data subject of the legal grounds for such refusal, in accordance with Article 20 of the GDPR.
Time limit for exercising the right to be forgotten	To comply with legal requirements, part of the information associated with certificates cannot be completely deleted, as it is necessary to ensure the legal validity of the certificates for a period of 7 years, as stated in Recital 61 of Regulation (EU) No.

Time limits for the storage of information	
	2024/1183. Therefore, when the data subject exercises the right to be forgotten, only the registration data will be deleted, with the following data excluded: • The data used to validate the identity of the certificate holder; • The certificate's private key (when applicable). This data will be securely encrypted and archived for a period of 7 years from the date of certificate issuance. After this period, all data will be automatically deleted. Requests for data deletion must be submitted in writing via the platform's Support area or sent to the following email address: dpo@acin.pt.
Time limit for reissuance of trust services approaching expiration date	All completed requests related to trust services will trigger an automatic reissuance request 45 days before their expiration date. If the subscriber does not complete the reissuance process, the original timelines for new requests will apply-payment, identity validation, and certificate generation.

4 USE RESTRICTIONS

Certificates issued by Global Trusted Sign are used by various holders, systems, applications, mechanisms, and protocols with the purpose of enabling probative signing of documents, emails, and transactions carried out by individuals or legal entities, as well as for encryption and access control. These certificates unequivocally ensure the identity of the holder, in accordance with the requirements of Regulation (EU) No. 2024/1183.

The subscriber:

- Agrees to comply with the terms and conditions of this agreement, in accordance with Global Trusted Sign's Certification Practice Statement and Certificate Policy (available at

<https://pki.globaltrustedsign.com> and <https://pki02.globaltrustedsign.com/>), as well as all applicable legislation.

- Agrees not to use the service for unlawful purposes, including but not limited to: disrupting the service; distributing content that infringes on privacy, intellectual property, or other third-party rights; or for any other purposes that Global Trusted Sign reasonably considers to be illegal, obscene, defamatory, fraudulent, abusive, threatening, harmful, or otherwise objectionable.
- Is solely responsible for the content of all transactions carried out through the service.

Documents and data submitted by subscribers located outside Portuguese territory must be issued by the official registry of the respective country, duly apostilled and officially translated into Portuguese or English.

Subscriber identity validation may be carried out in person (at the company headquarters in Madeira Island or at its facilities in Lisbon, Porto, and Ponta Delgada) or via videoconference, using certified electronic identification methods, in Portuguese or English, subject to prior scheduling and payment.

Subscribers with Portuguese identification documents can validate their identity through the authentication certificate of the Portuguese Citizen Card and/or Digital Mobile Key, via the portal autenticacao.gov.pt (available only to Portuguese citizens with compatible digital documents or certificates).

Identity validation is available on business days, from 09:00 to 17:30 (Madeira and mainland Portugal time).

With regard to SSL certificates, they focus exclusively on the identity of the certificate holder, not on their conduct. Therefore, a web authentication certificate does not guarantee that:

- The holder identified in the certificate is actually providing a service;
- The holder is in compliance with applicable legislation;
- The holder is trustworthy, honest, or ethical in conducting their business;
- It is “safe” to establish a business relationship with the certificate holder.

5 SUBSCRIBER RIGHTS

In accordance with the **General Data Protection Regulation (GDPR)**, as the data subject — subscriber of Global Trusted Sign — you have the following rights:

- To see what personal data Global Trusted Sign holds about you (**Art. 15 – Right of access**);
- To correct any inaccurate data (**Art. 16 – Right to rectification**);

- To restrict how your data is used (**Art. 18 – Right to restriction of processing**);
- To request the transfer of your data to another company, where technically possible (**Art. 20 – Right to data portability**);
- To request the deletion of your personal data (**Art. 17 – Right to erasure**);
- To request that Global Trusted Sign stop using your data for certain purposes (**Art. 21 – Right to object to processing**).

To exercise these rights, simply contact Global Trusted Sign. If your data is corrected, deleted, or its use is restricted, Global Trusted Sign will inform you accordingly (**Art. 19**).

Additionally, as a Global Trusted Sign subscriber, you also have the right to:

- File a complaint with the supervisory authority, the **Portuguese Data Protection Authority (CNPD) (Art. 77)**;
- Take legal action against the supervisory authority – CNPD (**Art. 78**);
- Take legal action against the data controller or processor (Global Trusted Sign – ACIN – iCloud Solutions, Lda), if necessary (**Art. 79**);
- Seek compensation and hold the controller liable if you suffer damage due to the unlawful use of your data (**Art. 82**).

6 SUBSCRIBER OBLIGATIONS

Responsibilities of the Subscriber/Certificate Holder

By accepting this service, the subscriber/certificate holder agrees to:

1. **Comply with the terms and conditions of this document**, as well as any specific conditions set forth in the agreement established with Global Trusted Sign.
2. **Use the certificates only for the permitted purposes**, in accordance with Global Trusted Sign's Certification Practice Statement and Certificate Policy (available at <https://pki.globaltrustedsign.com/> and <https://pki02.globaltrustedsign.com/>), and with applicable legislation.
3. **Not access, manipulate, or attempt to reproduce Global Trusted Sign's technical systems (hardware or software)**, unless prior written authorization has been granted.
4. **Provide accurate and up-to-date personal and professional information** at the time of registration, and inform Global Trusted Sign of any changes to that information.
5. **Verify that the private key associated with the certificate is valid and uncompromised** upon receiving the certificate.
6. **Notify Global Trusted Sign within a maximum of 24 hours** of any suspected misuse, unauthorized access, or unlawful behavior related to the certificate.

7. **Assume responsibility for any actions carried out with the certificate by representatives or employees.**
8. **Use the certificate solely in the role or function for which it was issued**, respecting the limits of representation.
9. **Inform Global Trusted Sign of any outdated data** and confirm that the information is up to date before requesting certificate reissuance.
10. **Follow all security procedures and technical requirements defined by Global Trusted Sign.**
11. **Immediately request certificate revocation** from Global Trusted Sign in the event of suspected security breach, loss of confidentiality, or any other reason for revocation as outlined in the Certification Practice Statement.

6.1 CERTIFICATE ISSUANCE PROCESS AND HOLDER IDENTITY VALIDATION

Before the certificate is issued by the holder, Global Trusted Sign is required to verify the identity of subscribers and holders, and, where applicable, other attributes, in accordance with Article 24(1) of Regulation (EU) No. 2024/1183 (eIDAS Regulation).

It should be noted that only in the case of advanced certificates, and where doubts arise concerning the documents submitted, Global Trusted Sign reserves the right to request identity validation, either in person or via videoconference (the latter subject to a fee of €10.00 + VAT), with the holder. For qualified certificates, identity validation must be carried out using one of the methods presented below.

The validation will be performed in compliance with the “requirements applicable to qualified trust service providers,” namely: *“when issuing certificates relating to trust services, qualified trust service providers shall verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom the certificate is issued.”*

Global Trusted Sign has mechanisms in place to validate the authenticity of all documentation submitted during the completion of the product purchase form, as well as to *“prove and verify the identity of natural or legal persons requesting the issuance of an electronic identification means.”*

The verification of the identity of subscribers and/or holders will be carried out by the registration authority administrators’ working group before the issuance of the qualified certificate and may be performed in the following ways:

- In person, in Portuguese or English, at the designated premises, upon presentation of the original identification document, [in accordance with point (a) of Article 24(1) of Regulation (EU) No. 2024/1183], or
- Via videoconference, in Portuguese or English, using certified software, by appointment. The physical presence of the individual or an authorized representative of the legal entity is required, with the presentation of the original ID document. This process must comply with Article 8 of Regulation (EU) No. 2024/1183, regarding “substantial” or “high” assurance levels, and GNS Order 154/2017 (per Article 24(1)(d));
- Using the authentication certificate of the Citizen Card and/or Digital Mobile Key, via the portal autenticacao.gov.pt, available only for Portuguese citizens with compatible digital certificates;
- Through a qualified electronic signature certificate issued in accordance with the previous clause (point d), paragraph 1, of Article 24 of Regulation (EU) No 2024/1183, applicable to reissues where the data remain unchanged and the holder maintains a valid certificate.

These identity validations can only take place after:

- a. Payment has been completed;
- b. The requested documentation has been submitted;
- c. All data has been reviewed and validated by registration officers.

To properly carry out identity validation, please take the following into account:

- I. In-person or videoconference validation (at Global Trusted Sign facilities in Madeira, Lisbon, Porto, or Ponta Delgada) is required by the Registration Administrator for the purposes of verifying the applicant's identity and the authenticity and adequacy of the submitted documents.
- II. For videoconference validations, ensure the following technical and documentation requirements are met:
 - a. Check your antivirus software for restrictions that may block the video call;
 - b. Use a recommended browser (Google Chrome or Firefox);
 - c. Provide a mobile number, as you will receive an activation code by SMS during the identity check;
 - d. Ensure the video call takes place in a well-lit environment, to verify the authenticity of your ID (e.g., Citizen Card with hologram);
 - e. Use a webcam and microphone of acceptable quality;
 - f. A mobile phone with camera and microphone may be used;

- g. Have your ID (e.g., Citizen Card with hologram) and the mobile number used to purchase the certificates at hand;
- h. If technical requirements are not met and a second videoconference is necessary, an additional fee of €10.00 will be charged;
- i. Videoconference validations are available on business days, from 09:00 to 17:30 (Madeira and mainland Portugal time).

Essential guidelines for a successful verification:

- a) Well-lit environment: Preferably with natural light to avoid shadows;
- b) Hold the document correctly: Use both hands without obstructing any information;
- c) Stable internet connection: Fast connection for high-quality video transmission;
- d) Follow instructions: Pay attention to timing and guidance during the videoconference;
- e) Glasses: If you wear them, remove them when requested for facial verification;
- f) Quality camera: Ensure clear image capture. We recommend using your mobile phone, as its camera typically provides better quality.

The videoconference is recorded for information security purposes. Consent is requested before and at the start of the recording. If this consent is not granted, the verification must be carried out in person at one of the locations provided by Global Trusted Sign for this purpose.

- I. If identity validation is performed via videoconference and the application forms are not digitally signed, the subscriber must send them via CTT (postal mail).
- II. The certificate issuance process will be completed on the date Global Trusted Sign receives the correctly completed and signed Certificate Issuance Form. G Global Trusted Sign will finalize the process within a maximum of 2 business days after receiving the documentation.

6.2 REISSUANCE OF CERTIFICATES

Reissuance applies to requests originating from previously issued certificates, provided that the data are maintained and remain valid and up to date.

If the holder wishes to reissue their certificate, they may use the request automatically created by the platform 45 days before the certificate's expiration date, or manually request reissuance with the same data, by following the instructions provided by Global Trusted Sign.

6.3DCS REVOCATION

Whenever a revocation request is submitted, its execution shall be carried out within a maximum of 24 hours, following the successful validation of the documentation provided (Form), including the duly completed and signed form.

6.4AMENDMENTS TO THE CERTIFICATE ISSUANCE FORM

These terms and conditions shall be amended accordingly if, during the period of validity of the form, new legislation is published or existing legislation is regulated, addressing matters covered by these General Conditions and imposing changes to the essential obligations of the parties, and if Global Trusted Sign deems it necessary to amend the terms of the Certification Practice Statement and the Qualified Certificates Policy that have been defined and/or contracted.

Global Trusted Sign will notify the holder about the contractual modifications, and its acceptance must be communicated by the holder within 30 days of such communication.

If the holder informs Global Trusted Sign the non-acceptance of the proposed amendments and being not possible to reach an agreement, any of the parties will be entitled to terminate this issuance form, and that denounce will take effects 60 days after the communication to the other party.

7 GLOBAL TRUSTED SIGN OBLIGATIONS

Global Trusted Sign, as a qualified trust service provider and data controller, ensures compliance with the principles of lawfulness, fairness, transparency, data minimization, storage limitation, proportionality, accuracy, security, and accountability.

8 OBLIGATIONS LIMITS

Global Trusted Sign is responsible for damages or losses caused to final users and relying parties arising from its activity, according to the applicable legislation.

Global Trusted Sign is not responsible for other damages or losses derived from abusive use or those uses outside the scope of the contract with users and/or relying parties.

Global Trusted Sign is not responsible for the failure of services related to cases of force majeure, such as natural disasters, war or similar events.

Global Trusted Sign reserves the right not to conclude a purchase process for digital certificates, when verified that the holder does not meet the requirements for the appropriate validation of the holder identity, being the applicant duly notified of the reasons.

The refusal to conclude the process, as long as it results from a cause not attributable to Global Trusted Sign, does not grant the holder the right to reimbursement of the amounts.

In particular, the holder will not be entitled to reimbursement of the amount paid for the certificate, if it is confirmed that he/she has provided false or incorrect information, or has omitted relevant information or documentation for the evaluation of the request, which is strictly necessary to continue with the process.

9 USE OF THE SERVICE

The holder of a public key certificate is only entitled to use the private key for the intended purposes (mentioned in the *KeyUsage* certificate field) within the law.

In the case of advanced certificates, the holder must authenticate on the G Global Trusted Sign portal and download their certificate through their user profile. To use the certificate, a PIN will be sent by SMS to the mobile phone number provided by the holder at the time of purchasing the product. The certificate may be downloaded as many times as necessary.

After login, the session remains active for a maximum period of 10 minutes without activity. After this time, the session is automatically terminated for security reasons, and a new login is required to continue using the platform.

The use of the certificate is only permitted, and when applicable according the type of certificate:

- To whom is mentioned in the *Subject* certificate field;
- While the certificate is still valid and is not included in the Certificate Revocation List (CRL) of the certification authority of Global Trusted Sign. This list is available at <https://pki.globaltrustedsign.com> and <https://pki02.globaltrustedsign.com/> and in the properties of the certificate as demanded by the applicable legislation.

The issuance and use of the certificate are always the responsibility of its holder.

Access to the Global Trusted Sign platform requires mandatory user registration, with authentication through personal credentials (username and password), as set out in these Terms and Conditions and in the Certificate Policy.

As a security measure, the use of strong passwords is recommended, as well as the configuration of two-factor authentication via Profile > Manage Account > Two-step verification.

10 PRICE AND PAYMENTS

ACIN – iCloud Solutions, Lda. reserves the right to update the prices charged annually, in accordance with the variation of the Consumer Price Index (CPI) published by the National

Statistics Institute, based on values not lower than the average CPI recorded in the immediately preceding year.

All payments shall be made in euros (€). The indicated amounts are subject to Value Added Tax (VAT) at the legally applicable rate.

11 SHARING INFORMATION WITH THIRD PARTIES

Global Trusted Sign has the right to share information with the competent authorities, provided that:

- It is obliged to do so by a subpoena, court order or any other judicial procedure of similar nature;
- It is necessary to comply with the legislation in force.

Global Trusted Sign subcontracts:

- PayPayUE – *Instituição de Pagamento, Unipessoal, Lda* – for the processing of payments via ATM, credit/debit card and MBWAY;
- the iGEST platform for invoicing, with the data shared being only that necessary to carry out this process;
- the Electronic IDentification platform, as regards videoconferencing for the validation of the identity of qualified electronic signature and qualified electronic seals service holders or when deemed necessary;
- autenticacao.gov.pt for authentication in the identity validation process of holders of Portuguese identification;
- the CRM - Salesforce, to manage support requests received by e-mail or telephone, as well as to manage sales leads.
- iDOK – Internal document management software used for archiving documentation sent and received by the parties.

Both parties — Global Trusted Sign and the holder/subscriber — have the right to retain evidence of the signed FO23 document, which must be kept on file for the legally required period for audit and compliance purposes.

12 PRESERVATION OF AUDIT LOGS

Audit records are retained for a period of seven years, as provided for in the applicable legislation.

13 AVAILABILITY OF SERVICES

CRLs can be checked at <https://pki.globaltrustedsign.com> and <https://pki02.globaltrustedsign.com/>, ensuring its availability 24 hours a day, 7 days a week, except in cases of any programmed maintenance stoppage, duly informed to the parties involved.

Global Trusted Sign has online certificate status OSCP validation services available at: <http://ocsp.globaltrustedsign.com>.

Furthermore, revocation requests will be processed in 24 hours. During that time interval, the identity and authenticity of the person who requested the certificate revocation will be verified. After confirming the identity and authenticity of the requester, Global Trusted Sign has 60 minutes to change the certificate status to revoked.

Revoked certificates can be checked in the CRL of the Certification Authority of Global Trusted Sign.

Global Trusted Sign does not guarantee the uninterrupted operation of the technological infrastructure that supports services mentioned in the Digital Certificate Issuance Form, in particular, when the infrastructure is subject to updates and improvements, required for the compatibility of Global Trusted Sign with possible legal or regulatory amendments, or with view to improve the complete operation of the infrastructure.

14 COMPENSATIONS

Global Trusted Sign will assume responsibility related to compensations, in accordance with the applicable legislation, in the terms set forth in Regulation (EU) No. 2024/1183 of the European Parliament and of the Council of 23 July 2014, and the General Data Protection Regulation 2016/679 of 27 April 2016.

15 CONTACTS

All stakeholders must use appropriate collective communications means. These means can include digitally signed electronic mail, fax, signed forms or similar, depending on the severity and on the subject.

Telephone calls are recorded for purposes of quality control, with the due authorization of the National Commission for Data Protection (*Comissão Nacional de Proteção de Dados* - CNPD). If you do not want your calls to be recorded, it is suggested to use alternative means.

Name	Global Trusted Sign Management Group
-------------	---

Managers	Tolentino de Deus Faria Pereira José Luís de Sousa
Address	ACIN iCloud Solutions, Lda. Estrada Regional 104 Nº42-A 9350-203 Ribeira Brava, Madeira Island – Portugal
General e-mail	info@globaltrustedsign.com
Report e-mail	report@globaltrustedsign.com
Website	https://www.globaltrustedsign.com
Phone Number	National: 707 451 451 ¹ International: + 351 291 957 888 ² (Global Trusted Sign - Option 3) ¹ Maximum price per minute: 0.09€ (+VAT) for calls originating on fixed networks and 0.13€ (+VAT) for calls originating on mobile networks; ² Cost of an international call to a fixed network, according to the tariff in force.

16 RIGHT OF WITHDRAWAL

The consumer has the right to withdraw from this contract within a period of 14 days, starting from the day following the date on which it was concluded, without having to provide any reason. After this period, the Right of Withdrawal expires.

For the purposes of exercising the Right of Withdrawal, the Client must express their intention through an unequivocal statement, which may be sent by post to Estrada Regional 104 No. 42-A, 9350-203 Ribeira Brava – Madeira, or by email to info@globaltrustedsign.com.

17 EFFECTS OF WITHDRAWAL

In the event of withdrawal from this contract, all payments made by the Client will be reimbursed without undue delay.

The refund will be made using the same payment method used by the Client in the initial transaction, unless expressly agreed otherwise.

Specificities of immediate performance of the contract and exercise of the Right of Withdrawal:

Given the nature and specific characteristics of the services to be provided, performance of the contract may, in some cases, begin immediately after it is concluded.

The Client therefore declares that they give their express consent for the services to begin before the 14-day period reserved for the Right of Withdrawal has elapsed.

The Client also acknowledges that if the services are fully performed before the end of that period, they lose the right to withdraw from the contract.

However, when the contract has not been fully performed and the Client, after having given the above-mentioned consent, exercises their Right of Withdrawal, they will be required to pay an amount proportional to the services provided up to the date the withdrawal is communicated.

18 CONTACT OF THE DATA PROTECTION OFFICER

In case of any doubt or any event related to data protection, Global Trusted Sign users may contact the Data Protection Officer (DPO – Art. 37, GDPR), appointed by the ACIN managers. These officers are available to provide support Global Trusted Sign customers and to cooperate with the appointed national control authority – National Commission for Data Protection (*Comissão Nacional de Proteção de Dados – CNPD*). These officers can be contacted by e-mail dpo@acin.pt or telephone, as indicated in point 14.

19 DISPUTE SETTLEMENT PROVISIONS

Complaints must be sent to the Global Trusted Sign Management Group, via registered mail.

The Portuguese law is applied when any dispute arises from the interpretation or implementation of this document. The parties choose exclusively the jurisdiction of the Judicial District of Funchal to settle such disputes.

Any dispute between users and Global Trusted Sign can be communicated to the Supervisory Authority, with the aim to settle any conflict that may arise.

20 APPLICABLE LEGISLATION

The following legislation applies to certification authorities providing trust services:

- a) Regulation (EU) No. 2024/1183 of the European Parliament and of the Council of 23 July 2024 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
- b) Other national and European legislation related to activities of provision of qualified trust services;
- c) General Data Protection Regulation 2016/679 of 27 April 2016.

Conformity audits will be regularly performed in Global Trusted Sign, pursuant the applicable legislation, by an external entity duly registered and acknowledged for that purpose, and its conclusions will be transmitted to the supervisory authority, which can make publicly known the conclusions of all the process, when requested.

I hereby declare that I have understood the content of these Terms and Conditions:

_____/_____,_____
(place), (day) (month) (year)

(Signature)