General conditions of subscription to the

Electronic Signature and / or Electronic Stamp service

SUBJECT

A. The purpose of these conditions is to specify the General Terms and Conditions of Subscription to the Electronic Signature service and/or Electronic Stamp provided by Worldline, as MediaCert TSP (Worldline Trust Service Provider) to its Subscribers.

B. It is specified that these Subscribers are:

- either Organizations acting for themselves, or on behalf of other Organizations which have mandated them for this purpose, to ensure, by issuing a Certificate in the name of their Organization, the Authentication of the origin of the Documents issued and the guarantee of their integrity (Certificate of Organization or Electronic Stamp);
- or Organizations who contract with Worldline to obtain Certificates, on behalf of Natural Persons who have authorized them to do so (employees, customers, etc.), referred to as "Holders" in this document, so that they can sign Documents electronically (Single-Use Certificate for creating OTU signatures);
- or Natural Persons acting on their own behalf, to ensure, by issuing a Certificate in their name, that they can sign Documents electronically (Permanent Certificate);

These Subscribers may, in addition, rely on Partners who are contractually attached to them, to distribute the Subscriber's offers to the Partners' own Customers. In this context, Subscribers are mandated by the Partners' own Customers to obtain the issuance of a Single-use certificate in their name that allows them to perform an OTU signature on Documents.

C. The distribution and management of Certificates, regardless of the type of Certificates (Single-use, Organizational or permanent), are governed by the Certification Policy - Declaration of Certification Practices for so-called "online" CAs, which is the responsibility of Worldline's MediaCert TSP. Throughout the document, the term "CP-CPS" will refer to the document referred to in this paragraph.

This CP-CPS is referenced under a public identifier structured as follows:

(OID): 1.2.250.1.111.20.5.v;

1.2.250.1: High level OID identifying AFNOR;

111: Worldline ID;

20: activity related to trust services;

5: number assigned to the CP-CPSs of the so-called "online" CAs;

v: CP-CPS version number.

The current OID of the CP-CPS of online CAs as of the date of publication of this document is:

(OID): 1.2.250.1.111.20.5.5

CP-CPS versions can be found at https://www.mediacert.com/

D. The CP-CPS of the online CAs has been evaluated by an independent audit firm to validate compliance with the ETSI standard for issuing electronic certificates at the Lightweight Certificate Policy (LCP) level. The ETSI standard used for the 2020 CA compliance audit is EN 319 411-1 as recommended, in the context of the application of European Regulation No 910/2014, for maintaining Certification at the LCP level.

1. DEFINITIONS

The following terms shall have the following meanings:

Subscriber: refers to the company signing the Subscription Contract attached hereto, registered in the Certificate Issuance Service produced by the Online Certification Authorities and wishing to obtain the delivery of its choice**:**

- Organizational Certificates "LCP" or "NCP" on behalf of Organizations that are dependent on the Subscriber or on behalf of Organizations that expressly mandate the Subscriber to do so;
- Permanent Certificates on behalf of Natural Persons, also called 'Subscriber', whose identification would have been previously checked;
- Standard" single-use Certificates in the name of the Holders whom it has previously identified or whose identification it has delegated, by contract to the conventional Attachments and under its responsibility, to identify.
- Reinforced" single-use Certificates in the name of the Holders whom it has previously identified or whose identification it has delegated, by contract to the conventional Attachments and under its responsibility, to identify.

The concepts of "standard" and "reinforced" for the qualification of Single-use certificates are specified in the following definition of **Registration Authority.**

Certification Authority (CA): the authority responsible for the application of the CP-CPS. The MediaCert TSP operates the so-called "online" CAs called:

- MediaCert OTU LCP CA 2018 and Mediacert OTU LCP CA S2 2019;
- Mediacert OTU CA 2019 and Mediacert OTU CA S2 2019 ;
- Mediacert ORG CA 2019 and Mediacert ORG CA S2 2019 ;
- Mediacert ORG NCP CA 2019 and Mediacert ORG NCP CA S2 2019 ;
- Mediacert PERM CA 2019 and Mediacert PERM CA S2 2019 ;
- AC OTU ;

which govern the five types of Certificates:

- The "standard" single-use certificates issued by the CAs MediaCert OTU LCP CA 2018 and Mediacert OTU LCP CA S2;
- The “Reinforced" single-use certificates issued by CA Mediacert OTU CA 2019 and Mediacert OTU CA 2019 S2 2019;
- LCP Organizational Certificates issued by the CAs Mediacert ORG CA 2019 and Mediacert ORG CA 2019 S2 ;
- NCP Organizational Certificates issued by the CAs Mediacert ORG NCP CA 2019 and Mediacert ORG NCP CA S2 2019;
- Permanent Certificates issued by the CAs Mediacert PERM CA 2019 and Mediacert PERM CA S2 2019.

Subscriber Initials

This document, the term "target CA" is used to refer to the CA that is designated according to the type of Certificate issued or to be issued.

The term also refers to the technical entities that issue Certificates at the request of the Registration Authority. They are responsible for the Certificates signed on their behalf and perform the following functions:

- monitor compliance with the current CP-CPS by the Registration Authority acting on behalf of the online CAs ;
- publish the public information referred to in chapter 2.2 of the CP-CPS, in particular these General Terms and Conditions of Subscription and the General Terms and Conditions of Services, in a sustainable and secure manner;
- ensure compliance with Worldline's Information Systems Security Policy by the various components of it;
- make its services accessible to any Subscriber who has accepted these General Terms and Conditions of Subscription;
- collaborate with auditors during compliance checks and implement any measures decided with auditors following compliance checks.

Throughout the document, the term "CAs" will refer to the so-called "online" CAs concerned by CP-CPS.

Registration Authority (RA): The authority responsible for receiving Subscriber Certificate applications, verifying these applications in accordance with the controls described in the CP-CPS based on the type of Certificate requested, archiving these applications and forwarding them to the target CA. The RA is also responsible for receiving and processing requests for Certificate Revocation.

For the purposes hereof, the responsibility for RA rests with the MediaCert TSP, which relies on the identity control commitments made by the Subscriber, directly or through its Contractually bound affiliates and which are described in the Subscriber's Identification Policy(s), which may differ depending on the context of issuing Single-use Certificates.

The issuance of Single-use Certificates requires that the Subscriber, directly or through its Contractually bound affiliates, has previously identified the applicants for this type of Certificate in accordance with the process described in the document entitled *"OTU Identification Policy and Procedures for Obtaining Consent"* provided in the form of a form by MediaCert TSP and that he has undertaken to complete and monitor. Such a document will be prepared for each journey of the same subscriber whose identification and/or consent conditions differ. As the identification process is described by the Subscriber, it is up to him to implement it or have it implemented under his responsibility. If persons are designated and authorized by the Subscriber to perform this identification under his responsibility, this must then be stipulated by the Subscriber in the identification policy he provides to the Registration Authority.

The "*OTU Identification Policy and Procedures for Obtaining Consent*" document described by the Subscriber had to be accepted, prior to its implementation, by the target CA and the RA when applying for a Subscription or when implementing a new route.

The identification policy follows the rules described in paragraph 3.2 "*Initial Identity Validation*" described in the CP-CPS and details the controls that will be implemented by the Subscriber, directly or through its agents or Partners with whom it has a contractual relationship, to respond to a reliable identification process for its Customers (Holders). In addition, depending on the level of identity control implemented, the Subscriber may be provided with a Single-use Certificate called:

- "standard": where the identity check of the future Holder complies with the requirements imposed by ETSI EN 319 411-1 level LCP;
-
- "reinforced": where the identity control of the future Holder complies with the requirements imposed by ETSI EN 319 411-1 level LCP **and** subject to additional requirements imposed by the CA.

The Registration Authority carries out random checks on the Subscriber, including his contractually bound affiliates, to verify compliance with the identification process described by the Subscriber.

Authentication: Authentication is an electronic process that confirms the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form. In short, to identify oneself is to communicate one's identity, to authenticate oneself is to provide proof of one's identity. *ANSSI - Agence Nationale de la Sécurité des Systèmes d'Information*.

Beneficiary of the Subscriber: the beneficiary is the person holding a right by virtue of his relationship, whether contractual or legal, with the Subscriber.

Electronic stamp: the "Electronic stamp" is a process used by an application service, thus differentiating itself from the "Electronic Signature" which is a dedicated term reserved for a natural person. The Electronic Stamp refers to data in electronic form, which is attached or logically associated with other data in electronic form to ensure the origin and integrity of the latter. It contains a timestamp corresponding to the production time of the Electronic stamp.

Certificate: electronic file issued by Worldline as trust provider service of MediaCert TSP.

According to the eIDAS Regulation:

- in the case of an "Electronic Signature certificate", means an electronic certificate that associates the validation data of an Electronic Signature with a natural person and confirms at least the name or pseudonym of that person;
- in the case of an "Electronic stamp certificate", means an electronic certificate that associates the validation data of an Electronic stamp with a legal person and confirms the name of that person.

The Single-use Certificate refers to a Certificate produced dynamically during an Electronic Signature process. This Certificate is used during a single signature session by the platform, then the signature key is destroyed. Its lifetime is limited to a few minutes in accordance with the applicable CP-CPS. This Certificate is generated at the Subscriber's request to perform a signature at the request of an End User on a Document.

In the context of a Single-use Certificate, by signing the Certificate, the CA validates the link between the identity of the natural person and the key pair.

The Electronic stamp certificate guarantees the origin of a message sent by a legal entity but is also used to encrypt exchanges, in order to ensure confidentiality, authentication and integrity. In this context, the Organization shall seal the Document in its name as identified in the Certificate, or in the name of the authorized representative of the Organization identified in the Certificate. The Certificate of Organization is requested by a representative authorized by the Organization.

This Electronic Stamp or Organization Certificate has a lifetime of several years, in accordance with the CP-CPS.

The Permanent Certificate is an Electronic Signature Certificate generated upon request of the Certificate Holder (natural person) to

the MediaCert TSP. Its lifetime is several years, in accordance with the CP-CPS.

These Certificates are signed by the online CAs of the MediaCert TSP established by Worldline.

Chain of trust: set of Certificates required to validate the filiation of a Certificate issued to an entity. CA trust chains are presented within CP-CPS.

Private Key: authentication, signature or encryption key, to be kept secret by the Certificate Carrier Device, which is associated with a public key contained in a Certificate.

Subscription Contract: refers to the subscription contract for the Electronic Signature and/or Electronic Stamp service. It consists of the documents referred to in Article 22, which form an inseparable whole.

Certificate Request: The Subscriber who wishes to apply for an Electronic Stamp Certificate or Organization Certificate must complete a document included in the Subscription File specifying in particular the contact details of the applicant(s) for such Certificate issued by the concerned CA.

The Subscriber who wishes to apply for a Single-use Certificate must present a request in electronic format. This request consists of a message (request) signed by the Subscriber and kept by the CA as justification for this request.

Certificate Carrier Device: a software component that obtains a Certificate(s) carrying the CA and guarantees the exclusive control of the two keys to the Certificate Holder and only to him. These Certificates are used according to the applications and types of Certificates for Electronic Signature purposes.

Document: electronic static document in PDF format.

Contractual Documents: all the documents referred to in Article 22 of the General Terms and Conditions of Subscription.

Personal identification data: a set of data used to establish the identity of a natural or legal person, or a natural person representing a legal person.

Registration file: all forms and supporting documents allowing the CA to justify the issuance and/or use of electronic certificates to perform Electronic Signatures or stamps on behalf of the Subscriber.

Evidence: as opposed to evidence (legal concept), evidence is used to refer to data and documents that are used to establish evidence. These may include computer traces, time stamp files, electronically signed files or any other document, file, which may be used by the Subscriber to demonstrate the existence and validity of the transaction carried out.

Electronic time stamping: data in electronic form that combines other data in electronic form at a particular time and establishes proof that the latter data existed at that time.

Identification: the act of establishing the identity of a natural or legal person or a natural person representing a legal person on the basis, in particular, of verified valid legal documents.

Electronic identification: the process of using personal identification data in electronic form that uniquely represents a natural or legal person or a natural person representing a legal person.

Service activity logs: all OTU service application logs (certificate production and signature/sealing).

Working Day: every day of the week except Saturdays, Sundays and public holidays.

List of Revoked Certificates (or CRL): list of serial numbers of Certificates that have been revoked. The url is visible in the Worldline Certificate.

Electronic identification means: a tangible and/or intangible element containing personal identification data and used to authenticate for an online service.

Organization: entity representing a company, a public administration, etc. or which may refer to a brand or company name for which an Organization Certificate or Electronic Stamp will be issued at the request of a Subscriber.

Online Certificate Status Protocol (OCSP): online certificate verification protocol, allowing the status of an X.509 digital certificate to be verified.

Route: functional kinematics leading to the OTU signature of one or more Documents. A Subscriber can define several routes. The paths are to be differentiated, in particular when the conditions for identifying cardholders are different, requiring the definition and validation by the RA of separate "*OTU Identification Policy and Procedures for Obtaining Consent*" documents.

Parties: Worldline or the Subscriber.

Certification Policy - Statement of Certification Practices (CP-CPS): a set of rules, identified by name (OID), defining the requirements with which a CA complies in the establishment and provision of its services and indicating the applicability of a Certificate to a particular community and/or class of applications with common security requirements.

CP-CPS describes from an organizational point of view the Worldline, through MediaCert TSP, service of providing Certificates and in particular their issuance, use and revocation process.

CP-CPS is available online: https://www.mediacert.com/

Reference: "WLM-OTU-F002".

Evidence Management Policy: a document that describes the policy followed by CAs to establish and maintain evidence of electronic exchanges. The Evidence Management Policy describes the rules, procedures, context for establishing and preserving Evidence in dematerialized services. It explains the security properties sought (integrity, authenticity, etc.) and the way they are ensured (Electronic Signature, time stamping, computer traces in particular).

OTU Identification Policy and Procedures for Obtaining Consent: a two-part document prepared by the Subscriber in support of Single-use Certificate applications, based on the *"WLF-OTU-F018"* form:

- the first part describes the procedures for identifying the Registrants, or end users, that the Subscriber implements or contractually delegates the implementation under his responsibility. On these identification processes depends the CA that will be targeted. The Identification Policy is subject to approval by RA after verification of compliance with the requirements described in paragraph 3.2.3.1 *"Validation of an Individual's Identity - Single-use Certificate"* of the CP-CPS;

- the second part details the process by which the Subscriber, directly or through its Contractually bound affiliates, can obtain the explicit and informed consent of the end user, prior to any request by the Subscriber for a Single-use Certificate on behalf of the end user. In particular, it sets out the actions to be taken before the OTU Certificate issuance process so that the Holder can give his agreement to the process implemented, give his consent to the Document presented to him and sign it electronically.

PDF: format of a computer file created by ADOBE Systems® and whose specificity is to preserve the formatting defined by its author.

Contractually bound affiliates: Partners or Organizations that are bound by contract with the Subscriber for the exercise by them of a number of obligations incumbent upon the Subscriber, such as the

application and compliance with the Identification Policy previously defined by the Subscriber, in return for their access via the Subscriber to the service for issuing Single-use certificates produced by the CAs. The Contractually bound affiliates must be expressly mandated by the Future Holders in order to be able to request a certificate from the Subscriber in their name. They may also be referred to as Beneficiary for the purposes of this document.

Authorized representative: refers to any natural person with the power to legally represent a subscribing company or an Organization. Proof of this authorization must be provided to RA.

Certificate Renewal: operation which consists in generating and making available a new Certificate for a Holder. There is no renewal in CAs for Single-use certificates.

Revocation: operation requested by the Certificate Carrier Device, the Subscriber's representative or one of the Subscriber's deputy representatives who has the identification and authentication data allowing him to access this function, or the MediaCert TSP (in accordance with the CP-CPS) to render a given Certificate invalid before the end of its validity period. The Certificate may become invalid for many reasons other than natural expiry, such as the loss or compromise of the Private Key associated with the Certificate or the change of at least one field included in the name of the Certificate Holder/Holder. The Revocation operation is considered complete when the serial number of the Certificate to be revoked and the Revocation date are published in the List of Revoked Certificates (CRL). The revocation of a certificate has no impact on the validity of Documents signed or sealed with this certificate in the period preceding its revocation.

Service: Certification service offered by Worldline as trust provider service of MediaCert TSP to the Subscriber to meet the needs of Electronic Document Signing.

Website: MediaCert TSP website dedicated to Services.

Signatory: a natural person who creates an Electronic Signature;

Electronic Signature: refers, in France, according to article 1367, paragraph 2, first sentence of the Civil Code below:

“the use of a reliable identification process guaranteeing its link with the act to which it is attached.”

According to Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014: data in electronic form, which are attached or logically associated with other data in electronic form and which the signatory uses to sign.

For the purposes hereof, the Electronic Signature does not constitute a qualified signature.

In the case of the use of an Organizational Certificate or Electronic Stamp Certificate, it is not an Electronic Signature of a natural person. The possible use of the term "Electronic stamp signature" should be understood as the application of a seal that guarantees the origin and integrity of a message.

Holder: a natural or legal person identified in the Certificate as the holder of this Certificate.

Definition Worldline MediaCert TSP

In the case of a Single-Use Certificate, the Holder is a Natural Person who has instructed the Subscriber to obtain the issuance of this type of electronic certificate to be able to sign (client, employee, etc.), or contractually bound affiliates authorized by the Holders to instruct the Subscriber to request a certificate on their behalf.

In the case of an Organization Certificate, the Holder is the Organization or a representative of the Organization. The generation and exclusive use of the Private Key associated with the public key indicated in the Certificate is entrusted to the "Certificate Carrying Device" entity.

In the case of a Permanent Certificate, the Holder is a Natural Person identified within the Mediacert TSP as a Subscriber, and having made a request of Certificate generation allowing to electronically sign Documents. The generation and exclusive use of the Private Key associated with the public key indicated in the Certificate is entrusted to the "Certificate Carrying Device" entity.

End User: refers to the natural person who has signed a transaction with the Subscriber, or Partners or Organizations, conventionally attached to the Subscriber and who uses the Electronic Signature Service offered by the Subscriber. The End User is the Holder of a Single-use Certificate.

The End User may benefit from the Electronic Signature Service provided that the following prerequisites are met:

- have the legal capacity to undertake to comply with the provisions applicable to the use of the service;
- have valid and up-to-date proof of identity to be able to identify themselves;
- possibly have, for certain Services, an e-mail address or a telephone number. In this case, this information must be active, accurate and personal.

2. PRECONDITIONS FOR THE CONSTITUTION OF SUBSCRIBER STATUS

2.1. Acceptance of the attribution of Subscriber status is based on a set of elements defined in Chapter 3.2.2.2.1 *"Validation of a Subscriber" of the* CP-CPS. This includes, in particular:

- the signature of a Subscription Contract (see Article22
- the appointment or appointment of Representatives within the Subscriber for Requests for the Creation of Single-use Certificates and/or Organizational Certificates;
- the delivery of a set of supporting documents.

2.2. In the event that an Organization is different from the Subscriber, the Subscriber must provide the RA with the information concerning the Organization as defined in section 3.2.2.2.2 *"Validation of an Organization"* of the CP-CPS.

2.3. The signing of the Subscription Contract entails recognition, in particular by the Subscriber, of the obligations contained in the Clause 8 and in the CP-CPS.

3. PRECONDITIONS FOR OBTAINING CERTIFICATES

To obtain Certificates, the Subscriber must complete the following formalities with RA:

3.1. The Subscriber must complete his Certificate Creation Request (ref. "*WLF-OTU-F007*"), in accordance with the service he has subscribed to from MediaCert TSP, depending on whether it is an Organization Certificate (or Electronic Stamp) and/or a Single-use Certificate and/or a Permanent Certificate.

3.2. The Subscriber shall be responsible for ensuring that the Certificates and/or the level of Electronic Signature chosen are appropriate to his needs and to the needs of his possible Contractually bound affiliates: before any request for the creation of a Certificate from the RA, the Subscriber shall be responsible for ensuring that the type of Certificate to be issued as part of the service is adapted to his internal delegation rules, his business needs and his legal constraints as well as those of his Contractually bound affiliates.

4. FOR THE ISSUANCE OF A CERTIFICATE OF ORGANIZATION

4.1. **Subscriber's file**. The Subscriber's file for the Electronic Stamp Service using Organization Certificates must be accompanied by supporting documents as described in paragraph 3.2 *" Validation of the applicant's authority"* in the CP-CPS.

Any incomplete file may be refused by RA. The information provided in the file must be complete, accurate and up to date. The Subscriber guarantees the verification of the information provided and the validity of the supporting documents accompanying it. Any modification of the information contained in the File must initiate the procedure for revocation of the certificate issued for any of the following reasons: death, departure or resignation of an Organization Certificate Holder. The RA reserves the right to refuse the File in the event that the Subscriber is insolvent, is the subject of legal proceedings or in any way violates public morals.

4.2. **Request for Certificates.** The Subscriber is responsible for verifying the information relating to the Subscriber provided and the validity of the supporting documents accompanying it, as well as for regularly updating such information. RA assumes no responsibility to the Subscriber for the form, accuracy, authenticity or legal effect of any supporting documents provided by the Subscriber. The Electronic Stamp or Organization Certificate produced by the CA is sent to the Subscriber for acceptance of the Certificate.

4.3. **Acceptance of the certificate.** Explicit acceptance of the information contained in the Certificate is required from either the Subscriber's legal representative who made the request or from the individual authorized by the Subscriber's legal representative identified in the Certificate. The formalism of this acceptance is detailed in the CP-CPS as well as in the e-mail notification of issuance of the Electronic Stamp Certificate or Organization sent by the issuing Certification Authority.

The Subscriber is required to notify MediaCert TSP in writing of any inaccuracies within ten (10) business days of the generation of the said Certificate, in particular in the event that the data entered on the Certificate does not correspond to the information contained in the Subscription File. In the absence of notification within this period, the Certificate shall be deemed to have been accepted. In the event of notification within the above-mentioned period, the RA shall decide on the provision of a new Certificate to the Organization.

4.4. The validity period of an Electronic Stamp, Permanent or Organization Certificate is defined in the CP-CPS and in this document, clause 1.

4.5. Two (2) months before the expiry date of the Certificate of Organization, a notification is sent to the Subscriber, inviting him to proceed with a new application for a Certificate of Organization. In the absence of a new request from the Subscriber, the service is interrupted when the certificate expires.

4.6. The new Certificate must be generated with a Private Key change.

5. FOR THE ISSUANCE OF A SINGLE-USE CERTIFICATE

5.1. **Subscriber's file.** The Subscriber file for the signature service using Single-use Certificates must be accompanied by supporting documents as described in paragraph 3.2.3.1 *"Validation of an individual's identity - Single-use Certificate"* in the CP-CPS.

In particular, it must contain the document "Identification Policy and Procedures for Obtaining Consent".

The Subscriber requesting the issuance of Single-use Certificates shall ensure, in accordance with the applicable CP-CPS, that the reliable identification procedures, recognized by the RA, of the future Holders of Certificates of this type, which it has previously described in the aforementioned document, are implemented or have implemented under its responsibility. The Subscriber guarantees the verification of the information provided and the validity of the supporting documents accompanying it. RA assumes no responsibility to the Subscriber for the form, accuracy, authenticity or legal effect of supporting documents provided by the Subscriber and the Holder(s).

Any Application whose Identification Policy does not provide the necessary controls to reliably identify clients, future Holders of Certificates of this type, will be refused by the RA.

5.2. **Request for Certificates.** In the case of Single-use Certificates, the Subscriber's e-mail message to request an RA Certificate (request) must include the information as described in Chapter 4.1.2.2.1 *"Processes and Responsibilities for Establishing a Certificate Application"* of the CP-CPS and must be electronically signed by the Subscriber.

The Subscriber acknowledges that the Certificate application to be issued in the name of the Holder will contain the following verified information relating to the Holder's identity: first name, surname, date and place of birth.

5.3. **Acceptance of the certificate.** Given the atomic nature of the signature operation in the context of the use of a Single-use Certificate, the validation of the data contained in the Certificate is carried out before it is issued.

5.4. The validity period of a Single-use Certificate is defined in the CP-CPS.

6. USE OF A CERTIFICATE OF ORGANIZATION

6.1. The use of such certificates must be in accordance with the applicable CP-CPS. Indeed, the Subscriber undertakes to use the Certificates issued by the CA only for applications that allow the use of an Organizational Certificate as described in CP-CPS in paragraph 1.5 "*Certificate Uses*". In the event of a breach of this obligation, Worldline, through the MediaCert TSP, cannot be held liable.

6.2. In the context of Electronic Stamp or Organization Certificates, the Subscriber authorizes the CA to use the Private Key attached to the Certificate for the purpose of implementing Electronic stamps.

6.3. The user must check, at least before use, the information on the status of the certificate he intends to use in accordance with the intended use. It may, for this purpose, use the various means made available in accordance with paragraph 4.9.6.2 *"Requirements for verification of revocation by users of Certificates - Organization or Permanent Certificate"* of the CP-CPS.

7. USE OF A SINGLE-USE CERTIFICATE

7.1. The use of such certificates must comply with the applicable CP-CPS. Indeed, the Subscriber undertakes to use the Certificates issued by the CAs only for applications that allow the use of a Single-use Certificate as described in paragraph 1.5 "*Use of Certificates*" in the CP-CPS. In the event of a breach of this obligation, Worldline cannot be held liable.

7.2. The Subscriber, including its contractually bound affiliates, acknowledges that the implemented Electronic Signature kinematics must be clearly presented to the end user. This end user must be able to accept it before it is implemented and at the same time give the Subscriber a mandate to request a Single-use certificate for him/her in order to be able to sign the Document(s) presented to him/her.

8. REVOCATION OF A CERTIFICATE OF ORGANIZATION OR PERMANENT

8.1. **Origin of the Revocation.** The authorized persons or entities are described in paragraph 4.9.2.2.2 *"Origin of a request for Revocation - Certificate of Organization or Permanent"* of the CP-CPS.

8.2. **Cause of the Revocation.** The reasons for revocation are described in paragraph 4.9.1.2 of the CP-CPS *"Possible Causes for Revocation - Certificate of Organization or Permanent*".

8.3. **Responsibility.** Under no circumstances shall Worldline, through the MediaCert TSP, be held liable if an authorized representative of the Subscriber has not requested the revocation of the Electronic Stamp Certificate when one of the circumstances described in the aforementioned paragraph of the CP-CPS, of which he is aware, occurs.

8.4. **Revocation procedure.** The Procedures for processing a revocation request are described in section 4.9.3.2 of the CP-CPS *"Procedure for Processing a Revocation Request - Certificate of Organization or Permanent*".

The revocation of an Organization Certificate leads to the generation of a List of Revoked Certificates. The number of the Certificate concerned by the revocation request is then entered in the List of Revoked Certificates.

The concerned CA then publishes this list of revoked Certificates to the address defined in paragraph 4.10 *"Certificate Status Information Function"* of the CP-CPS.

Users of this type of Certificate can view this list without limitation.

8.5. **Confirmation of the revocation.** The MediaCert TSP will confirm, in the context of a request for revocation of this type of Certificate, by e-mail to the applicant that the request for Revocation of the Certificate has been executed.

9. REVOCATION OF A SINGLE-USE CERTIFICATE

9.1. **Origin of the Revocation.** The authorized persons or entities are described in paragraph 4.9.2.1 *"Origin of a request for Revocation - Single-use certificate"* of the CP-CPS.

9.2. **Cause of the Revocation.** The reasons for revocation are described in paragraph 4.9.1.1.1 of the CP-CPS *"Possible causes of revocation - Single-use certificate*".

9.3. **Responsibility.** Under no circumstances shall Worldline, through the MediaCert TSP, be held liable if an authorized representative of the Subscriber has not requested the revocation of the Single-use Certificate when one of the circumstances described in the aforementioned paragraph of the CP-CPS, of which he is aware, occurs.

9.4. **Revocation procedure.** The Procedures for processing a revocation request are described in section 4.9.3.1 of the CP-CPS *"Procedure for processing a revocation request - Single-use certificate*".

The revocation of any Certificate leads to the generation of a List of Revoked Certificates. The number of the Certificate concerned by the revocation request is then entered in the List of Revoked Certificates.

The concerned CAs then publish this list of revoked Certificates to the address defined in paragraph 4.10 *"Certificate Status Information Function"* of the CP-CPS.

Users of this type of Certificate can view this list without limitation.

9.5. **Confirmation of the revocation.** As the Revocation request is automatically authorized, the Holder concerned is informed of the change in status of his certificate via the publication of the List of Revoked Certificates at the addresses defined above.

10. SUBSCRIBER COMMITMENTS

10.1. Provision of documents by the RA Subscriber.

Certificate of Electronic Stamp or Organization

The Subscriber must provide the Registration Authority with:

- the document of Request for Creation of an Electronic Stamp Certificate or Organization Stamp provided by an authorized Subscriber's representative if he/she wishes to create such a certificate;
- documentary evidence supporting the content of the Certificate to be produced by the CA;
- and in particular, in the event that the name of the Organization to be included in the Certificate is different from that of the Subscriber:
- a valid proof (mandate) from the legal or authorized representative of the Organization in question allowing the Subscriber to request the issuance of a Certificate on behalf of that Organization;
- any document, valid at the time of the request for the creation of the Certificate, attesting to the existence of the Organization (extract from KBIS dated less than three (3) months ago or, original or copy of any official deed or extract from the official register dated less than three (3) months ago attesting to the name, legal form, registered office address and identity of the partners and corporate officers mentioned in 1° and 2° of Article R. 123-54 of the Commercial Code or their equivalents under foreign law, etc.);
- all supporting documents necessary to support the credentials of the representative of this Organization if the natural person representing this Organization is not the legal representative of this Organization (valid and not revoked delegation of power) and proof of the membership of this natural person in the Organization.

It is specified that it is the Subscriber's responsibility to check the validity and completeness of the documents he provides to the Registration Authority when applying for a subscription.

Permanent Certificate

The Subscriber must provide the Registration Authority with :

- the Permanent Certificate Creation Request document fully completed;
- information and documentary evidences (or copies) of the Subscriber's identity, supporting the content of the Certificate to be produced by the CA;

It is specified that it is the Subscriber's responsibility to verify the validity and completeness of the documents that it provides to the Registration Authority at the time of its subscription request.

Single-use certificates

The Subscriber must provide the RA, which must validate it, with the document "*Identification Policy and Procedures for Obtaining Consent*" completed by himself and/or by his beneficiaries with his assistance and under his responsibility.

This document contains:

- a written description of the process for identifying Single-use Certificate Holders. The identification process must include the presentation of a document or a copy of an identity document of the Holder and controls to certify the validity of the document, either before or during the Electronic Signature process;
- the procedures for obtaining consent must describe the process by which the Subscriber can obtain the explicit and informed consent of the end user on a number of points prior to any request on his behalf for a Single-use Certificate;
- among the items subject to the consent of the Holder, include in particular:
    - the Holder's acceptance to give the Subscriber the authority to initiate a request to the CAs to obtain a certificate on behalf of the Holder;
    - the Holder's explicit consent for the CAs to collect and process its data for the purpose of providing it with an electronic certificate and to retain it for the purpose of fulfilling their obligations to the Auditors.
    - the Holder’s explicit consent to generate a certificate on its behalf.
    - the Holder’s agreement to the General Conditions of Service of Electronic Signature Service, delivered beforehand

Subscriber Initials

10.2. **General obligation of the Subscriber to inform the Holders.** The Subscriber guarantees to inform the end user, in his capacity as Holder, in accordance with the obligations described in his Subscription Contract. In this respect, the Subscriber guarantees to provide, prior to any action by the end user, the information necessary for his understanding of the terms and conditions of the contractualization procedure, in particular online:

- by informing him/her about the kinematics of expressing his/her consent, the Electronic Signature process used and by explaining the legal consequences of his/her various actions, including in particular the processing by the target CA of his/her personal data;
- by informing him/her about the content of the evidence gathered and by indicating who is the service provider for the management and conservation of evidence;
- by informing it of its possibility of abandoning the procedure it has initiated;
- by informing him/her of the possibility of withdrawal or not;
- by informing it of the procedures for making the Contractual Document it has signed available to it, the procedures for keeping it;
- by inviting them to consult the General Terms and Conditions of Online CA Services available online at: https://www.mediacert.com/.

10.3. **Verification of Certificate Creation Requests.** The Subscriber is required to verify the accuracy and completeness of the information provided to the RA in the signed electronic message (request) or in the paper form intended for the Registration Authority and which is necessary for the issuance of either the Single Use Certificate or the Organization Certificate by the CAs.

10.4. **Non-discriminatory practices.** The Subscriber further undertakes not to engage in discriminatory practices in the services it provides that could be detrimental to those provided by the CAs.

10.5. **Compliance with obligations by the holder(s) of Single-use certificates.** The Subscriber also undertakes to ensure that the Registrants comply with the provisions applicable to them and resulting from his Subscription Contract.

To this end, it will ensure in particular that the Agreement Attachés comply with these provisions vis-à-vis the Holders.

The Certificate must be used in accordance with the provisions of the CP-CPS in force.

10.6. RA Information by the Subscriber

Electronic Stamp or Organization Certificates

The Subscriber must:

- to inform the Registration Authority in the event that the data in the Certificate is no longer valid due to a change within the Organization. In this respect, the Subscriber must notify the RA without delay, by registered letter with acknowledgement of receipt:
- any change in the identity of the person acting as Subscriber's representative or Deputy Subscriber's representative, as well as the effective date of such change, together with supporting documents;
- any changes in the information provided to RA, as well as the effective date of these changes.
- to communicate as soon as possible to the Registration Authority any event that may affect the reliability of the means of authentication with the latter. In this respect, changes (first name, surname, e-mail address) must be notified to the RA;
- to inform the Registration Authority in the event that the Organization no longer exists. In this respect, the Subscriber must notify the RA without delay, by registered letter with acknowledgement of receipt, of any changes (first name, surname, e-mail address, Organization ID) affecting all the Organization's Certificates, accompanied by supporting documents;

  to inform the Registration Authority in the event that information concerning the Organization, not included in the Certificate of Organization and having no impact on its validity, is modified. In this respect, the Subscriber must notify the RA as soon as possible, by simple letter, of any changes in information.

Permanent Certificates

The Subscriber shall:

- notify as soon as possible the Registration Authority of any change in contact information (address, e-mail);
- inform the Registration Authority in case the data in the Certificate is no longer valid due to a change in the name.

Single-use certificates

The Subscriber is responsible for:

- communicate as soon as possible to the Registration Authority any event that may affect the quality of the identification of its future Registrants;
-
- communicate as soon as possible to the Registration Authority any event that may affect the reliability of its means of authentication with the latter.

11. WORLDLINE'S COMMITMENTS

11.1. Worldline undertakes to implement the necessary means (technical and human) to provide the Services. The level of service implemented is that set out in the contract referred to in the Subscription Contract attached to these General Terms and Conditions.

11.2. Worldline, through MediaCert TSP, undertakes to use the keys generated exclusively to produce the Electronic Signature(s) necessary to complete a transaction requested by the Subscriber.

11.3. Worldline, through MediaCert TSP and the Certificate Carrier Device, undertakes to use the Private Key of the end user or the Organization only for the purposes intended by the CP-CPS.

11.4. Worldline, through MediaCert TSP, undertakes to authenticate any request from the Subscriber for a Certificate request and undertakes to keep proof of this request.

11.5. Worldline, as MediaCert TSP, keeps all the data necessary for the CAs defined in Chapter 5.5.2 *"Archive Retention Period"* of the CP-CPS, including:

- registration files:
- eight (8) years for files concerning Single-use Certificates;
- ten (10) years for files concerning Organization or Permanent Certificates.
- service activity logs: ten (10) years.

11.6. Worldline as the MediaCert TSP, has a duty to advise the Subscriber so that he can choose in an informed way, the technical solution of Electronic Signature adapted to the type of signature

path he has determined. MediaCert TSP involvement is limited, as part of a best efforts obligation, to a technical service that allows the Subscriber or his or her beneficiaries to benefit from the Electronic Signature and/or Electronic Stamp Services on Documents in accordance with the applicable CP-CPS. Worldline has no control over the content of the Documents subject to the services provided by MediaCert TSP, other than the insertion of Electronic Signatures and/or Electronic Stamps and does not access the content of the Documents to provide its services. Worldline cannot be held liable for the value or validity of the content of the Documents.

12. SERVICE INTERRUPTION

The Subscriber acknowledges that Worldline, as MediaCert TSP, may interrupt the Service, in whole or in part, in order to maintain or improve it. MediaCert TSP shall inform the Subscriber as soon as possible of any planned interruption (in particular by e-mail or by information on the Website) and shall limit the duration of the interruption and its impact on the Service.

13. PROOF AGREEMENT

The Parties expressly agree that in the context of their contractual relations, dated electronic messages shall constitute proof between them. The parties agree that as soon as a message is transmitted electronically from a sender to a recipient, the recipient is deemed to have received it by return of acknowledgement of receipt.

14. FINANCIAL CONDITIONS

MediaCert TSP does not market the Certificates alone, but only in addition to higher level services provided by itself or by sub-companies. These services are specified in the contract referenced in the Subscription Contract associated with the present General Terms and Conditions.

This contract details all the financial conditions.

15. RESPONSIBILITY OF THE SUBSCRIBER AND- GUARANTEED BY HIM/HER

Responsibilities

15.1. The Subscriber remains solely responsible to Worldline, in its capacity as MediaCert TSP, for the proper completion of the Holder identification and Authentication steps and for ensuring that the choice of Electronic Signature process meets its needs and those of its potential Contractually bound affiliates.

15.2. In the event that Worldline, in its capacity as MediaCert TSP, does not receive the supporting documents collected by the Subscriber including those collected by the Contractually bound affiliates, in support of the identification of the Holders, MediaCert TSP carries out a sampling campaign of Single-use signatures made at the Subscriber's request in order to verify the correct application by the Subscriber, including its Contractually bound affiliates, of the Identification Procedure validated jointly between the parties. Sampling must make it possible to verify that the identity check has been carried out and requires that proof of this check has been kept for a minimum period of eight (8) years by the Subscriber, including his Contractually bound affiliates. This sampling campaign shall take place at least once (1) a year. In the event of deviations from this procedure, the Subscriber undertakes to establish an action plan with Worldline to resolve such deviations. Non-application of this action plan or the discovery of discrepancies during the next sampling campaign may lead to the deactivation of the Electronic Signature service using Single-use Certificates for the Subscriber, including his beneficiaries, in accordance with the provisions mentioned in the CP-CPS.

Guarantees

15.3. The Subscriber indemnifies Worldline, as MediaCert TSP, against any action, claim or demand that may be brought against it by a Holder or a third party, and any damage resulting therefrom, arising directly or indirectly from or based on the failure of the Subscriber, his beneficiaries or a Holder to comply with any of the provisions of the Subscription Agreement, including the documents relating thereto.

15.4. The Subscriber, including its conventional affiliates, guarantees MediaCert TSP in general that the content of the documents transmitted by it and/or its conventional affiliates is lawful and does not allow acts contrary to applicable and current laws and regulations to be carried out.

15.5. The Subscriber undertakes not to make any commitment in the name and on behalf of the MediaCert TSP, which it may under no circumstances replace.

16. WORLDLINE'S LIABILITY AND WARRANTY

Responsibilities

16.1. Worldline provides a technical service by providing the Subscriber with the Electronic Signature and/or Electronic Stamp Services of the MediaCert TSP.

16.2. The Subscriber acknowledges that MediaCert TSP has no influence on the content of the Documents issued by it, except for the insertion by the CAs of MediaCert TSP of Electronic Signatures or Electronic Stamps on said Documents and may not therefore be held liable for the content and information they contain.

16.3. Worldline's liability is limited to direct material damage to the exclusion of any indirect damage. In the event that Worldline, as a Trust Service Provider, is held liable, it is expressly agreed that Worldline may only be held liable for compensation up to an amount that does not exceed the amount specified in the Service Agreement, the references of which are specified in the Subscription Agreement for the Electronic Signature and/or Electronic stamp service (ref. *"WLF-OTU-F005*") attached to these General Conditions.

16.4. Worldline assumes no responsibility for the consequences of any delays, alterations or losses that the Subscriber may suffer in the transmission of any electronic messages, letters or documents.

16.5. Worldline shall not be held liable in the event of total or partial interruption of the Service in accordance with Article 12 above.

16.6. Trust ¨Provider MediaCert TSP can only be held liable in the event of proven non-compliance with its obligations.

16.7. The MediaCert TSP may not be held liable in the event of a fault in the scope of a Subscriber entity, in particular in the event of:

- use of an expired certificate;
- use of a revoked certificate;
- use of a certificate in an application other than those described in Chapter 4.5 *"Use of the Key pair and Certificate"* of the CP-CPS.

16.8. MediaCert TSP is generally not responsible for the documents and information provided by the Subscriber and does not guarantee their accuracy or the consequences of harmful facts, actions, negligence or omissions of the Subscriber, his representative or the Holder.

16.9. In the event that Worldline is held liable as a Certification Authority in the event of a breach by the Subscriber, including all its beneficiaries, of one of the obligations imposed on them, the Subscriber shall subrogate itself to Worldline for any dispute settlement or legal action that may result from it originating from a Beneficiaries, a User or a third party.

16.10. **Absolute necessity.** Worldline shall not be held liable for any loss, damage, delay or failure to perform obligations resulting from the General Terms and Conditions when the circumstances giving rise to them are due to force majeure within the meaning of Article 1148 of the French Civil Code. The Parties further agree that the following shall be considered as force majeure: decisions of a public authority, legislative and/or regulatory changes, acts of unpredictable third parties that have caused damage making it impossible to provide the Service. In the event that the case of force majeure prevents one of the Parties from fulfilling its obligations for a period of more than two (2) months, each of the Parties may terminate the Subscriber Agreement, automatically and without

legal formality, without the Subscriber being entitled to claim any compensation.

Guarantees

16.11. Worldline, as MediaCert TSP, warrants to Subscriber that the services provided are in compliance with the applicable CP-CPS available on the MediaCert TSP Website on the day of use of the Service;

16.12. Worldline cannot replace the Subscriber in the choice of the level of service subscribed in connection with the legal regimes applicable to Business Documents for which the Subscriber has decided to use Electronic Signature and/or Electronic Stamp.

16.13. Consequently, the provision of the Service by Worldline shall not exempt the Subscriber from analysis and verification of the legal or regulatory requirements in force relating to such Business Documents.

16.14. MediaCert TSP undertakes to issue certificates in accordance with the CP-CPS concerned, as well as with the state of the art and technology.

16.15. MediaCert TSP guarantees through its services:

- the Subscriber's authentication with his certificate by the Registration Authority;
- the generation of certificate(s) in accordance with the Subscriber's request, previously authenticated and verified;
- the provision of information functions on the status of certificates issued, following the Subscriber's request, by CAs in accordance with this document;
- the exclusive control of the Private Key of the Certificate by the Certificate Carrier Device and the destruction of the same key after a single session of use in the case of a Single-use certificate.

17. MODIFICATION OF DOCUMENTS AND CONTRACTUAL CONDITIONS

Documentary developments due to external constraints

17.1. **General Terms and Conditions of Subscription.** The General Terms and Conditions of Subscription, which are intended to evolve to take into account legal, technical or commercial constraints, will be updated.

In this case, the MediaCert TSP shall modify or update these General Terms and Conditions by simply updating the content to take these changes into account.

The MediaCert TSP will notify, via a signed e-mail, of any updates to the General Terms and Conditions of Subscription as soon as possible.

This notification shall specify the effective date of such updates.

17.2. **CP-CPS and/or the General Terms and Conditions of Services.** In the event of a change affecting the CP-CPS and/or the General Terms and Conditions of the current Online CA Services, Subscribers will be informed, via a signed e-mail, at the latest one (1) month before the publication of the new version of the amended document in accordance with the change affecting it. This notification shall specify the effective date of such updates.

17.3. Any notification between the parties shall be validly made to the Subscriber at his e-mail address indicated in his registration file or at any other address that the parties may subsequently communicate to each other by ordinary mail or e-mail.

17.4. In the event of a change that is likely to have a major impact on the Subscriber and/or Worldline and its Organization, such updates shall be notified to the Subscriber in accordance with paragraph 9.11 *"Individual Notifications and Communications between Participants" of* the CP-CPS.

17.5. The updated documents will also be available and accessible online as soon as they come into force at the following address: https://www.mediacert.com/.

17.6. The Subscriber, including his or her beneficiaries, is informed that he or she may save and/or print the applicable General Subscription Conditions.

17.7. **Documentary developments due to the MediaCert TSP.** Changes made to a Contractual Document at the initiative of the MediaCert TSP shall be brought to the attention of the Subscriber by any means, at least one (1) month before their entry into force.

17.8. **Other developments.** If any changes required in the service should have an impact on the economy of the contract referred to in the Subscription Contract, the Subscriber will then have the possibility to terminate his contract in the event of disagreement, without any penalty at his expense. In the absence of termination and if the Holder(s) continue to use the service or Certificate(s) at the end of the above period, the Subscriber shall be deemed to have accepted such changes.

18. DURATION

The Subscription Agreement takes effect from the date of its signature by the Subscriber for an indefinite period, without however exceeding the duration of the higher level service contract referred to in the Subscription Agreement.

19. TERMINATION

19.1. The Subscriber Agreement may be terminated, ipso jure and without legal formality, by registered letter with acknowledgement of receipt, by the Subscriber or the Certification Authority:

- for convenience, following compliance with the notice period stipulated in the Contract referenced in the Subscription Contract;
- without notice, in the event of a breach by the other party of any of its contractual obligations, if the breach has not been remedied within one (1) month of a formal notice by registered letter with acknowledgement of receipt (1st presentation) which has remained without effect;
- in the event of force majeure, under the conditions described in Article16.10 of this document;
- ipso jure, in the event of termination of the Service Agreement to which this Subscription Agreement is linked.

19.2. In the event of termination of the Subscription Contract and on the effective date of termination, access to the Subscriber's service, including its beneficiaries, will be cut off and any electronic Seal Certificates issued will be immediately revoked without the Subscriber being able to assert any right to compensation.

19.3. The Subscriber is prohibited from requesting the creation of a Certificate from the Registration Authority on the effective date of the Termination.

20. INTELLECTUAL PROPERTY

The provision of a Certificate does not confer any ownership rights on the Subscriber or Holders over the Certificate.

21. PROTECTION OF PERSONAL DATA

21.1. **Electronic Stamp or Organization or Permanent Certificates.** The personal data collected as part of this Subscription Contract are mandatory for the processing of the registration file. They are intended, as well as those that may be collected subsequently, for CAs that are authorized by the Subscriber, duly authorized for this purpose, to store them in computer memory, use them, and communicate them for the same purposes and under the same protection, to Worldline legal entities or to third parties authorized

for the purposes of managing Electronic Stamp and Permanent Certificates.

21.2. **Single-use certificates.** In the context of Single-use certificates, it is recalled that the Subscriber will ensure that he/she obtains the express acceptance of the future Holders, before transmitting the personal data of these future Holders to the Registration Authority, for the processing of requests to create Certificates of this type.

To this end, the future Holder must agree that the personal data concerning him/her collected by RA from the Subscriber may be processed electronically for the sole purpose of:

- constitute its identification and allow its authentication in order to generate a certificate in its name;
- be able to communicate to him the activation data of his Private Key;
- make it possible to support the identity indicated in the Certificate by providing the necessary proof, if necessary, by keeping the elements in the registration file;
- to support its obligations as a trusted third party.

It is indeed specified that any opposition to the retention of personal data will prevent the issuance of this type of Certificate. Indeed, by accepting the provision of the Certificate to proceed with an Electronic Signature, the Holder accepts that the CA via the RA, retains, at the request of the RA, the personal data for the duration necessary to fulfil the purposes of the processing operations carried out in the context of the provision and management of the Single-use Certificate.

21.3. The Subscriber, including representatives of Subscribers or Organizations and Holders, have the right to access, rectify, delete and object to their personal data communicated, which they may exercise by contacting Worldline at the address indicated below:

Comité MediaCert
Worldline
23, rue de la Pointe
Zone Industrielle A
59113 Seclin
France
dl-mediacert-tsp@worldline.com

21.4. This right of rectification, deletion and opposition must not, however, prevent the right to keep data enabling proof of a right or contract to be established for as long as the purpose for which the data are stored so requires.

21.5. Worldline has implemented and complies with personal data protection procedures to ensure the security of data transmitted by:

- the Subscriber, including all his Contractually bound affiliates;
- the Holders, natural persons, to the Subscriber, including all of its conventional affiliates, who communicates them to Worldline under this contract for the purpose of identifying and authenticating them.

It is the Subscriber's responsibility to obtain from the Holders, natural persons, their consent for the personal data concerning them collected by the Subscriber - for the purpose of identifying and authenticating them, to be transmitted by the Subscriber to the RA and the CA for computer processing, in order to allow the RA and the CA to issue Certificates on behalf of the Holders, so that the Holders can sign the Documents presented by the Subscriber online. It is specified that the personal data communicated by the Contractually bound affiliates to the Subscriber to be transmitted by the Subscriber to the RA and CA must, in the same way, have been subject to the same authorization and consent procedures, in such a way that the RA and CA may process them.

21.6. The Holders must guarantee on their honour to the Subscriber, including their Contractually bound affiliates, the accuracy of the data they transmit for this purpose. Holders must be informed of their rights to have their information rectified in the event of a change in this information.

21.7. The Holders must be informed of the nature of the information concerning them, which is kept by the RA and CA as part of the implementation of the MediaCert TSP services and give their prior consent to the processing.

21.8. The Holders must be informed of the elements traced on behalf of the Subscriber to provide proof of electronic exchanges, if necessary. This information is detailed in the Evidence Management Policy, available on electronic request (e-mail).

21.9. The Parties undertake to comply with the provisions of the Data Protection Act of 6 January 1978 n°78-17 relating to computer science, files and liberties. As such, each Party undertakes to ensure the security of personal data when it is transmitted to the other Party, regardless of the transmission medium used in accordance with the aforementioned law.

Each Party is responsible for its own files and assumes full responsibility for the processing applied to them.

21.10. The Parties undertake to comply with the laws applicable to them.

The Parties shall ensure compliance with the obligations contained in this Article by all their staff, their agents or Contractually bound affiliates and any other person for whom they are responsible.

21.11. The obligations contained in this article shall apply for the duration of this Agreement and without limitation after its expiry.

21.12. The Parties agree to provide each other with all information necessary for the proper conduct of the operations processed, in particular in accordance with the Data Protection Act and the GDPR.

22. CONTRACT DOCUMENTS

22.1. The Subscription Contract consists of the documents, which form an inseparable whole, listed below:

- the membership contract for the Electronic Signature service and/or Electronic Stamp;
- the present General Terms and Conditions of Subscription to the Electronic Signature and/or Electronic Stamp Service;
- the *"OTU Identification Policy and Procedures for Obtaining Consent"* in the case of subscription to the OTU Electronic Signature service;
- the Certification Policy – Certification Practices Statements available online at the address defined in Article1

In addition, it is part of the process of granting Subscriber status as defined in Article2.1 this document.

22.2. All the above-mentioned documents constitute the technical framework within which the Subscriber's Electronic Signature service will be carried out. It is supplemented by the provisions of the higher-level Service Agreement, which specify in particular Article14 these Terms and Conditions, Article18 on duration and Article16 on Worldline's Liability.

In the event of any inconsistency between the articles of the General Terms and Conditions of Subscription and those of the provisions of the higher-level Service Agreement, the clauses of the General Terms and Conditions of Subscription which are based on the applicable Certification Policy - Certification Practices Statements shall prevail.

23. APPLICABLE LAW

It is specified that the interpretation, validity and execution of this Agreement are subject to French law.

Subscriber Initials

The MediaCert TSP, offering the services covered by these General Terms and Conditions, in all its components and including documentaries, is governed by the laws and regulations in force in the French territory applicable to it, although its activities arising from the CP-CPS associated with these General Terms and Conditions may have legal effects outside the French territory.

In addition, only the French version of the contractual documents, listed in Article22.1 this document, is enforceable against the parties, even in the presence of translations. Indeed, the translations of express agreements are provided for mere convenience and cannot have any legal effect, in particular on the interpretation of the Subscription Contract or the common intention of the parties.

24. DISPUTE SETTLEMENT

In the event of a dispute relating to the interpretation, formation or execution of this contract and failing to reach an amicable agreement, any dispute will be brought before the competent courts of Paris.

Subscriber Initials