

## Terms of Use (Workspace)

The purpose of these general conditions of use applicable to the Workspace (hereinafter the "**Workspace General Conditions of Use**" or "**WGCU**") is to define the conditions of access and use of the Services offered by Cryptolog International, RCS Paris n° 439 129 164 (hereinafter "**Universign**") to its Customers who create and manage Workspaces under their responsibility, and to Users who are invited to use them by a Customer.

### DEFINITIONS

Unless otherwise stated, capitalized terms have the meaning attributed to them in this article and may be used in the singular or plural, depending on the context.

**API:** refers to the computer interface enabling access to the Service.

**Certification Authority (CA):** refers to the authority in charge of creating, issuing, managing and revoking Certificates in accordance with the Certification Policy.

**Preservation Authority (PA):** refers to the authority in charge of preserving Electronic Signatures, in particular by means of checks on these elements and methods for extending the reliability of Signatures beyond their technological validity period.

**Time-Stamping Authority (TSA)** means the authority responsible for issuing Time-Stamps under the Time-Stamping Policy.

**Electronic Seal:** refers to the process used to guarantee the integrity of a sealed Document and to identify the origin of this Document by means of the Certificate used for its Sealing.

**Customer:** means a natural or legal person who creates, configures or exclusively manages a Workspace as part of their professional activity in order to use one or more Service(s) and who (i) has accepted the Universign Saas Terms and Conditions, or (ii) has signed a specific commercial agreement with Universign or one of its Partners to use one or more Service(s).

**User Account (personal account):** refers to the computer resources allocated by Universign to a User wishing to use one or more specific Services. Each User Account (personal account) is linked to the User's e-mail address.

**User Account (Workspace):** refers to the computer resources allocated by Universign to a User wishing to use one or more Workspaces. Each User Account (Workspace) is linked to a single e-mail address of the User.

**General Terms and Conditions of Use for Personal Accounts (or CGUCP):** refers to the general terms and conditions of use applicable to Users wishing to benefit from specific Services. They are available on the Website.

**Preservation:** refers to the associated Service consisting of the implementation of procedures and technologies enabling the reliability of Electronic Signatures to be extended for a specified period.

**Time marker:** designates a structure that links a Document to a particular time, establishing proof that it existed at that time.

**Electronic Document or Document:** refers to all structured data that can be processed by the Service.

**Documentation:** refers to the functional and technical documentation provided by Universign in connection with the use of the Services.

**Registration file:** refers to the file on which the Certificate application is based, containing the information and supporting documents required by the Certification Policy.

**Workspace:** refers to the computer resources allocated to the Customer by Universign, enabling the Customer to invite Users to use the Services.

**Time-Stamping:** refers to a process which, by means of Time-Stamps, makes it possible to certify that a Document existed at a given time.

**Identifier:** refers to the specific characters with which each User connects to the Service.

**Updates:** refers to successive versions of the Platform containing technical and/or functional improvements, provided by Universign. Updates include all modifications made to the Platform to bring it up to date with regulatory changes and changes affecting the operating environment.

**Delegated Registration Operator or DRO** means a User who carries out Certificate holder registration operations on behalf of and on the instructions of Universign, and is therefore responsible for verifying the identity of the Certificate holder in his presence (with a "face-to-face") and for compiling his Registration File.

**Partner** means a natural or legal person who integrates or markets one or more Universign Services with the solutions it publishes, in order to make them available to a Customer.

**Platform:** refers to the technical infrastructure comprising all the hardware, software packages, operating system, Updates, databases and environment managed by Universign or its subcontractors on which the Software Package will be operated. It enables the Software Package to be supplied in SaaS mode. It is directly accessible remotely via the Internet directly on the Website or by means of a smartphone or touch tablet.

**Certification Policy (CP):** refers to the set of rules, identified by a number (OID), defining the requirements to which a CA conforms in setting up and providing its services.

**Preservation Policy (PP):** refers to the set of rules with which the HA complies to implement the Preservation Service.

**The Personal Data Protection Policy or PPDP** provides information on the personal data processed by Universign as part of the Services, the purposes and basis of such processing, the sharing of such data with third parties and the rights applicable to Users who have transmitted such data.

**Validation Policy (VP):** refers to the set of rules to which the VA conforms for the implementation of the Signature and Seal Validation Service.

**Time-Stamping Policy or TSP** means the set of rules with which the TSA complies for the implementation of the Time-Stamping Service.

**Subscriber:** designates the person, physical or moral, identified in the Certificate who has under his control the private key corresponding to the public key.

**Software Package:** refers to a set of programs, procedures and rules, and possibly Documentation, relating to the operation of an information processing system. The Software Package is developed by Universign to make the Services available in SaaS mode.

**Validation Report:** refers to the document issued by Universign following analysis of the Signature or Stamp of a signed or sealed document.

**SaaS (Software as a Service):** refers to the mode of access to the Service. This access is made remotely via the Internet by connecting to the shared Platform hosted on the servers of Universign and its subcontractors.

**Electronic Seal or Sealing:** refers to a process that guarantees the integrity of the sealed Document and identifies its origin by means of the Certificate used for sealing.

**Service(s):** refers to all services and software solutions in SaaS mode that Universign undertakes to provide to the Customer.

**Signatory:** refers to the natural person wishing to conclude or having concluded a Transaction with a User by means of the Service.

**Electronic Signature or Signature:** refers to a process used to guarantee the integrity of the signed Document and to express the consent of the Signatory it identifies.

**Website:** refers to the <https://www.universign.com> website.

**Storage:** refers to the service associated with the Universign Electronic Signature Service, consisting of the possibility of storing Documents signed using the Service on the Platform.

**Universign Support:** refers to Universign web support available via the URL <https://help.universign.com/>.

**Transaction:** refers to the process between the Customer and a third party during which an Electronic Document proposed by the Customer using the Service is signed or time-stamped.

**User:** means a natural person who is a member of at least one Workspace, and who has an account with specific rights and obligations depending on his or her role, in order to use the Services for professional purposes. The User using a Service within a Workspace acts under the contractual responsibility of the Customer who is at the origin of its creation.

## **ARTICLE 1 - PURPOSE**

These Customer Terms and Conditions define the conditions applicable to the Services accessible by the Customer via the Website or API.

## **ARTICLE 2 - CONTRACTUAL DOCUMENTS**

The Contract concluded between Universign and the Customer consists of the following contractual documents, presented in hierarchical order of decreasing legal value:

- The policies relating to the subscribed Services published on the Website ;
- As the case may be, the Universign General Terms and Conditions of Sale or the applicable specific commercial agreement.
- The PPDP

- The present CGUET ;

- The CGUCP if applicable.

In the event of contradiction between one or more stipulations contained in the above-mentioned documents, the higher-ranking document shall prevail.

Universign reserves the right to modify these GTUET at any time and without notice.

The CGUET are permanently accessible on the Website.

### **ARTICLE 3 - ACCEPTANCE**

Prior to any use of the Service, the Customer acknowledges that he has read the GTUET and accepts them unreservedly.

The Customer's acceptance of this agreement is evidenced by clicking on the checkbox on the Website when creating a Workspace.

He therefore acknowledges that his commitment does not require a handwritten or electronic signature.

### **ARTICLE 4 - WORKSPACE**

#### ***4.1. - Creating a workspace***

Access to and use of the Service require the creation of a Workspace.

The Workspace is created by the Customer, who can configure one or more Workspaces and designate one or more Users within the limits of the rights subscribed.

Each User has more or less extensive rights depending on his or her profile.

By default, the customer has a Workspace owner profile with extended rights.

The Customer may create one or more Workspaces in order to benefit from a Service, subject to having :

- Suitable computer equipment to access the Service;

- A valid, personal e-mail address (access to which is controlled by the user)

#### ***4.2. - Access to the Workspace***

To access the Workspace, the Customer is required to authenticate himself using the Identifier he has freely determined when creating his first Workspace.

The Customer Identifier is strictly personal. It must meet the security criteria set by Universign and must not under any circumstances be communicated to third parties.

It is expressly reminded that Universign will never, for any reason whatsoever, ask the Customer to provide its Identifier and that any such request will be considered as a fraudulent request.

The Customer is entirely responsible for the safekeeping and use of his Identifier. They must take all necessary measures to prevent unauthorized or fraudulent use of their Workspace(s).

If the Customer observes or suspects any unauthorized or fraudulent use of its Identifier or those of the Users of its Workspace or any other breach of security, it must immediately alert Universign via the Universign Support service.

Upon receipt of such notification, Universign will proceed within a reasonable time to deactivate the User Account (Workspace) concerned.

#### ***Article 4.3. - Inviting Users to a Workspace***

The Customer may invite one or more Users to the Workspace he owns.

User access to a Workspace requires prior acceptance of the CGUET.

Any access to the Workspace by a User is carried out under the responsibility of the Customer who configured it. The Customer is responsible for all actions carried out by Users of its Workspace, including access to and use of the Service via the API, and releases Universign from all liability in the event of damage caused to a third party by such actions.

#### ***Article 4.4. - Use of the Workspace***

The Customer undertakes to ensure that Users of its Workspace provide Universign with accurate information for the use of the Service. The Customer ensures that Users refrain from any abnormal, abusive or fraudulent use of the Service. In particular, the Customer undertakes to ensure that Users access the Service via the API in accordance with the Documentation.

In general, the Customer undertakes to ensure that Users refrain from any activity using the Service that is in breach of the laws and regulations applicable to it.

Failure to comply with the conditions of use of a Service from a Workspace is the sole responsibility of the Customer, without prejudice to the immediate deactivation of a User Account (Workspace) or any liability action that Universign reserves the right to take.

#### ***Article 4.5. - Closing a Workspace***

The customer may decide to close the Workspace he has created from the Universign solution.

### **ARTICLE 5 - USER ACCOUNT (WORKSPACE)**

#### ***5.1. - Creating a User Account (Workspace)***

The Workspace is created by the Customer, who may designate one or more Users within the limits of the rights subscribed to.

Therefore, the creation of a User Account (Workspace) is required in the following two cases:

- the User is a Customer and has created a Workspace
- the User has been invited by a Customer to the Workspace he has configured.

Each User has more or less extensive rights, depending on the Profile assigned to him by the Customer.

The User may create a User Account (Workspace) to use a Service, provided that he or she has :

- Suitable computer equipment to access the Service;
- A valid, personal e-mail address (access to which is controlled by the user)

#### ***5.2. - Access to the User Account (Workspace)***

To access the User Account (Workspace), the User is required to authenticate using the User ID freely determined when creating the User Account (Workspace).

The User's Identifier is strictly personal. It must meet the security criteria set by Universign and must not under any circumstances be communicated to third parties.

It is expressly reminded that Universign never asks the User, for any reason whatsoever, to communicate its Identifier and that any such request will be considered as a fraudulent request.

The User is entirely responsible for the safekeeping and use of his/her User ID. He/she must take all necessary measures to prevent unauthorized or fraudulent use of his/her User Account (Workspace).

If the User or Customer observes, suspects or becomes aware of any unauthorized or fraudulent use of a User Account Identifier (Workspace) or any other breach of security, they must immediately alert Universign Support.

Upon receipt of such notification, Universign will proceed within a reasonable time to deactivate the User Account (Workspace) concerned.

Any access to a User Account (Workspace) by a User is carried out under the Customer's responsibility. As such, the Customer is responsible for all actions carried out by Users of its Workspace, including access and use of the Service via the API, and releases Universign from all liability in the event of damage caused to a third party by such actions.

### ***Article 5.3. - Closing a User Account (Workspace)***

Closure of a User Account (Workspace) may be by the Customer or any User with appropriate functional rights.

## **ARTICLE 6 - SERVICES PROVIDED**

### ***6.1. - Service delivery and development***

The Services are delivered in SaaS (Software as a Service) mode. They are regularly updated to improve their quality and/or existing functionalities for all Users.

Universign reserves the right to add to or modify the Service at any time in line with technological developments, and will inform Users by any means.

Such Updates shall be considered part of the Service and shall be subject to the terms hereof.

You are advised to consult the Website regularly for information on any changes.



Universign reserves the right, without prior notice or compensation, to temporarily restrict access to the Service, in particular to carry out Updates, maintenance operations, modifications or changes to operating methods or access times, without this list being limitative.

Universign is not responsible for damages of any kind that may result from these changes and/or from the temporary unavailability of the Website, API or Service.

## ***6.2. - Service quality***

Universign endeavours to provide a Service that complies with the current policies available on the Website.

Due to the nature and complexity of the Internet network, and in particular its technical performance and response times for consulting, querying or transferring information data, Universign cannot guarantee absolute availability of the Website, the API and, more generally, the Service.

Universign cannot be held responsible for the proper functioning of the User's computer or telephone equipment, or for the User's access to the Internet or to a mobile telephone network.

The User is responsible for the telecommunication costs of his Internet connection operator when using the Service.

## **ARTICLE 7 - SPECIFIC CONDITIONS OF USE OF SERVICES**

The stipulations described in this article describe the specifics applicable to each of the Services provided via the User Account (Workspace). In the event of contradiction with the general stipulations included in the other articles, the specific conditions per Service described in the present article will prevail for each Service concerned.

### ***7.1. - Time-stamping service***

The Service enables Documents to be time-stamped by means of Time-Stamped issued in accordance with the Time-Stamping Policy, which describes in greater detail the implementation and organization of the Service.

#### **7.1.1. Service access**

The Signatory can benefit from the proposed Service on condition that it has :

- A User Account (Workspace).

Use of the Service via the API requires configuration of the User's information system in accordance with the Documentation.

#### 7.1.2. Use of the Service

The User sends the Document to be time-stamped to the Service, via the Universign API, in accordance with the Documentation.

In response to the User's request, the Service sends a Time-Stamp, the components of which are described in the Time-Stamping Policy.

#### 7.1.3. Service description

The Service shall not be used to establish proof that an e-mail has been transmitted to or received by a recipient. The Service does not constitute an electronic registered mail service. The Service may not be used for the purpose of identifying the author or origin of the Document.

#### 7.1.4 Warranties and warranty limits

Subject to compliance by Customers and Users with the CGUET and applicable policies, Universign guarantees the enforceability, within the meaning of European regulations, of Time Marks created using the Service.

The Time-Stamping performed using the Service benefits from a presumption of the accuracy of the date and time contained in the Time-Stamp and of the integrity of the Document to which this Time-Stamp relates.

The Time-Stamping Service is synchronized with Coordinated Universal Time so that the accuracy of Time-Stamps is one (1) second.

In the event of an event affecting the security of the Service and which could have an impact on Time Marks, appropriate information will be made available to Users via the Website.

Universign does not guarantee the suitability of the Service for the needs of the Customer and Users. It is the User's responsibility to verify this suitability, in particular by ensuring that the provisions of the Time-Stamping Policy meet their own requirements.

#### 7.1.5. Obligation of the User

The User undertakes to check the validity of Time-Stamps as soon as they are received, in accordance with the verification procedure described in the Time-Stamping Policy.

The information required to implement the Time-Stamp verification procedure described in the Time-Stamping Policy is available on the Website.

Apart from the cases provided for in the Time-Stamping Policy, Time-Stamps may be verified for a period of five (5) years from the date of issue.

The User also undertakes to check that the time-stamped Document is indeed the one sent to Universign for time-stamping.

The archiving of Time Marks is the sole responsibility of the User.

7.1.6. Data retention

In accordance with the Time-Stamping Policy and applicable regulations, Universign retains event logs relating to the operation of the Service for a period of six (6) years.

7.1.7. Policies and standards

Universign undertakes to comply with the policies and standards set out in the following table.

1.3.6.1.4.1.15819.5.1.1	ETSI EN 319 411-1	Time-Stamping Authority PC
1.3.6.1.4.1.15819.5.2.2	ETSI EN 319 421	Time-Stamping Policy

These Policies are published on the Website. They are audited by an accredited body in accordance with standard EN 319 403.

**7.2. - Electronic Stamping Service**

The Service enables the use of Electronic Stamps, the legal effects of which are recognized by the regulations applicable in the territory of the European Union.

7.2.1. - Service access

Access to the Service requires :

- A User Account (Personal Account) ;
- A User Account (Workspace)

- A Certificate of a legal entity associated with cryptographic keys that comply with one of the Certification Policies mentioned herein.

Access to the Service using the API requires configuration of the User's information system in accordance with the Documentation.

Documentation is provided by Universign upon request of the User after creation of his User Account (Workspace).

#### 7.2.2. - Use of the Service

The User sends the Document to be sealed to the Service, via the API, in accordance with the Documentation.

In response to the User's request, the Service sends the Document to which an Electronic Seal has been affixed.

#### 7.2.3. - Limits of use

The Service enables an Electronic Seal to be affixed to a Document. It must not be used to establish proof of the consent of the Subscriber of the Certificate used for the Electronic Seal. The Electronic Seal does not constitute an Electronic Signature within the meaning of European regulations.

#### 7.2.4. Electronic stamp categories

##### *7.2.4.1. Level 1 electronic stamp*

Category 1 Electronic Stamps are created using Certificates that comply with the requirements of the ETSI EN 319 411-1 standard, which notably provides for the possibility of remote verification of the Subscriber's identification data.

##### *7.2.4.2 Level 2 electronic stamp*

Category 2 Electronic Stamps are created using qualified Certificates that comply with the requirements of ETSI EN 319 411-2, which stipulates in particular that the Subscriber's credentials must be verified in the presence of his or her expressly authorized representative.

##### *7.2.4.3 Level 3 electronic stamp*

Category 3 Qualified Electronic Stamps are created using Qualified Certificates that comply with the requirements of ETSI standard EN 319 411-2, which stipulates that the Subscriber's credentials must be verified in the presence of his or her expressly authorized representative.

7.2.5. Guarantees and limits of Guarantees

Subject to compliance by Customers and Users with the CGUET and applicable policies, Universign guarantees the enforceability, within the meaning of European regulations, of Electronic Stamps created using the Service.

Universign does not guarantee the suitability of the Service for the User's needs. It is the User's responsibility to verify this suitability, in particular by ensuring that the provisions of the Certification Policy meet his own requirements.

The User undertakes to provide Universign with accurate information for the use of the Service.

7.2.6. - Obligations of the User

The User also undertakes to check that the sealed Document is indeed the one sent to Universign for the creation of an Electronic Seal.

The archiving of sealed Documents is the sole responsibility of the User.

7.2.7. Data retention

Universign keeps event logs relating to the operation of the Service for a period of fifteen (15) years from the date of sealing.

7.2.8. Policies and standards

Universign undertakes to comply with the policies and standards set out in the following table:

<b>1.3.6.1.4.1.15819.5.1.3.4</b>	<b>ETSI EN 319 411-1</b>	<b>PC for legal entity certificates, LCP level</b>
1.3.6.1.4.1.15819.5.1.3.5	ETSI EN 319 411-2	PC for legal entity certificates, QCP-1 level

Next

These policies are published on the website. They are audited by an accredited body in accordance with standard EN 319 403.

### **7.3. - *Electronic Signature Transaction Management Service***

The Transaction Management Service provides Users with a solution for creating an Electronic Signature, enabling them to collect it from one or more Signatory(ies).

#### 7.3.1. Service access

Access to the Service requires the creation of a User Account (Workspace).

It can be done either via the API or via the Website.

#### 7.3.2. Service description

The User undertakes to provide Universign with accurate information for the use of the Service.

The Electronic Document Signature process is based on the following steps:

##### Step 1: Document availability

A User, via a Workspace, makes the Document available to the Signatory for signing and, where applicable, reading.

##### Step 2: Invitation to sign

The User completes the Signatory data required by the Service.

##### Step 3: Access to the signed document

Access to the original signed Document is available via the Customer Workspace.

#### 7.3.3. Limits of use

The User undertakes not to misuse the functionalities of the Service or the means of authentication of the Signatory, in particular by entering information relating to the Signatory which he knows to be incorrect or by not allowing the Signatory to correctly view the Document to be signed or entering the confidential code sent to the Signatory himself.

Any use of the Service that does not comply with these terms and conditions may render the Electronic Signature unenforceable and/or invalidate the document to which it is affixed.

#### 7.3.4. Electronic Signature Levels

The Service enables the implementation of three levels of Electronic Signature, the legal effects of which are recognized by the regulations applicable in the territory of the European Union.

##### *7.3.4.1. Level 1 electronic signature*

When implementing the Level 1 Signature, Universign cannot guarantee the identity of the Signatory or his credentials. Signatory identification is the responsibility of the Customer, using its own organizational and technical processes, which it implements under its sole responsibility.

Universign authenticates the Signatory by means of the Signatory's telephone number declared to Universign (by the Signatory himself or by the Customer), where applicable.

Level 1 Electronic Signature does not require the Signatory to create a User Account (personal account).

When using this Signature, Universign cannot guarantee the identity of the Signatory, the only elements provided being those communicated by the User.

The identification data appearing on the Electronic Signature are those transmitted by the User to Universign.

##### *7.3.4.2. Level 2 electronic signature*

As part of the implementation of the level 2 Electronic Signature, the Signatory's identification is checked remotely by means of the digital copy of his identity document sent to Universign.

Universign authenticates the Signatory by means of the Signatory's telephone number declared to Universign (by the Signatory himself or by a User), where applicable.

When using this Signature, Universign cannot guarantee the identity of the Signatory. Consequently, it is the Customer's responsibility to implement organizational or technical processes to ensure that Users of its Workspace verify the identity of the Signatory by their own means and under their sole responsibility.

Universign checks that the identification data declared is consistent with the proof of identity, a copy of which has been sent to Universign.

Level 2 Electronic Signature is performed using Certificates that comply with the requirements of ETSI EN 319 411-1.

Level 2 Electronic Signatures require the issuance of a Certificate for which the Subscriber is the Signatory.

#### *7.3.4.3. Level 3 electronic signature*

As part of the implementation of level 3 Electronic Signature, Universign or an OED verifies the identity of the Signatory in his presence and by means of proof of identity.

Universign authenticates the Signatory by means of the Signatory's telephone number declared to Universign (by the Signatory himself or by the User), where applicable.

Level 3 Electronic Signature is performed using Qualified Certificates that comply with the requirements of ETSI EN 319 411-2.

Level 3 Electronic Signatures require the issuance of a Certificate for which the Subscriber is the Signatory.

#### *7.3.4 Warranties and warranty limits*

As part of the implementation of the level 3 Electronic Signature, Universign guarantees the use of a Qualified Certificate, the issue of which is subject to verification of the Signatory's identity by appropriate means and in compliance with French law.

Subject to Users' compliance with the CGUET and applicable policies, Universign guarantees the enforceability, within the meaning of European regulations, of Electronic Signatures created using the Service.

Universign in no way verifies that the Service corresponds to the legal regimes applicable to the Documents. Consequently, the provision of the Service does not exempt Users from analysis and verification of applicable legal and/or regulatory requirements.

#### *7.3.5. Document storage*

Unless otherwise specified by the Customer, Universign stores the Documents signed using the Service in such a way as to preserve their integrity. Storage enables the Customer and the Users of its Workspaces to consult the signed Documents online, to keep them, to return them and/or to destroy them.



The function of the Electronic Preservation service is to guarantee, for the duration of the Storage, the integrity of the signed documents and to extend the reliability of the Electronic Signatures beyond their technological validity period.

Universign reserves the right to store signed Documents with a specialized subcontractor.

Where Storage is carried out by Universign and unless otherwise agreed between Universign and the Customer, the Documents are stored from the time they are deposited until the occurrence of one of the following events:

- Fifteen (15) years after the filing date of the Document ;
- Manual deletion of a Document from the Workspace by a User
- Closing the Workspace ;
- Two (2) months after the end of a Contract unless a reversibility period extends it;

It is the Customer's responsibility to take all necessary steps to ensure that Documents which are no longer or not stored in a Workspace by the Service are preserved in a durable and integral manner.

#### 7.3.6 User obligations

Each User agrees that :

- the content of the Documents is lawful and does not permit illegal acts or acts contrary to applicable laws and regulations;
- the content of the Documents does not infringe the privacy of individuals and/or provisions relating to the protection of personal data and/or competition law and/or consumer law

Use of the Service outside these guarantees is the sole responsibility of the Customer.

#### 7.3.7 Customer obligations

The Customer undertakes to :

- Where applicable, if acting in a commercial or professional capacity, that he/she complies with the obligations incumbent upon him/her in respect of his/her status, particularly in terms of compulsory information and the transmission of signed Documents,

-implement all technical, legal and organizational measures enabling it to ensure proper use of the Services by Users of its Workspaces

#### 7.3.8. Limitation of liability

Universign does not control the content of the Documents, and therefore cannot be held liable for the value and/or validity of the content of the Documents or for any defect therein.

Universign cannot be held responsible for the consequences of any decisions made or actions taken on the basis of these Documents (whether signed or not).

Universign cannot be held responsible for inappropriate use of the Service with regard to the regulations applicable to Documents.

#### 7.3.9. Policies and standards

Universign undertakes to comply with the policies and standards set out in the following table.

1.3.6.1.4.1.15819.5.1.3.3	ETSI EN 319 411-1	PC for LCP-level certificates for natural persons
1.3.6.1.4.1.15819.5.1.3.1	ETSI EN 319 - 411 - 2	PC for certificates of natural persons, level 1

Next

These policies are published on the Publication Site. They are audited in accordance with EN 319 403 by an accredited body.

#### 7.3.10. Proof file

For signatures, Universign will provide Users with the data extracted from its event logs to help establish proof of the operations constituting an Electronic Signature, subject to the production of one or other of the appropriate supporting elements, in accordance with the existing procedure which may be communicated to Users on request to Universign Support.

The Customer authorizes Universign to communicate to any Workspace User the proof file inherent in a signed Document.

These data will be transmitted in the form of a file attesting to the authenticity of these data and sealed by means of an Electronic Certificate in the name of Universign.

The Court Evidence Files will be stored for a period of 15 years from the date on which the Document is signed by all the Signatories.

#### **7.4. - Conservation service**

The Preservation Service extends the reliability of Electronically Signed Documents beyond their technological validity period, in accordance with the Preservation Policy, which describes in greater detail the implementation and organization of the Service.

##### 7.4.1. Service access

Access to the Service is an option integrated into the Electronic Signature service provided by Universign.

It requires suitable computer equipment to access the Service and a User Account (Workspace).

The Service is provided by default to all Customers storing electronically signed Documents with a Universign solution.

It can be deactivated at the Customer's request.

##### 7.4.2. Use of the Service

When electronically signed documents are stored at Universign, the latter uses its solution to process them in such a way as to ensure the reliability of the signatures they contain beyond their technological validity period.

The Service then integrates all the elements described in the Preservation Policy into the electronically signed Document.

##### 7.4.3. Limits of use

The Service does not constitute an electronic archiving service, in particular with regard to the NF Z42-013 standard.

##### 7.4.4 Warranties and warranty limits

Universign also guarantees to provide a Service that complies with the Preservation Policy.

Universign does not guarantee the suitability of the Service for the Customer's needs. It is the Customer's responsibility to verify this suitability, in particular by ensuring that the Services and the provisions of the Preservation Policy meet the Customer's specific requirements.

Use of the Service outside these guarantees is the sole responsibility of the Customer.

7.4.5. Document storage

It is the User's responsibility to take all necessary steps to store Documents that have been Preserved, as these Documents are not stored by the Service.

7.4.6. Data retention

Universign keeps event logs relating to the operation of the Conservation Service for a period of fifteen (15) years.

7.4.7. Limitation of liability

Universign does not control the content of the Documents processed within the framework of the Services, and therefore cannot be held liable for the value and/or validity of the content of the said Documents or for any defect in the latter.

Universign cannot be held liable for the consequences of any decisions made or actions taken on the basis of these Documents, the reliability of which has been extended beyond the period of technological validity.

7.4.8. Policies and standards

Universign undertakes to comply with the policies and standards set out in the following table.

1.3.6.1.4.1.15819.5.8.1	ETSI TS 119,511	PP for extension storage of signed documents
1.3.6.1.4.1.15819.7.4.1	ETSI TS 119,511	PLR for extension storage of signed documents
1.3.6.1.4.1.15819.5.8.2		Conservation Profile
1.3.6.1.4.1.15819.5.8.3		Proof of Preservation Policies

Next

These policies are published on the Publication Site. They are audited in accordance with EN 319 403 by an accredited body.

### **7.5. - Signature Validation and Electronic Stamp Service**

The Signature and Seal Validation Service enables a User to validate a previously operated Signature or Seal.

#### 7.5.1. Service access

Access to the Service requires the creation of a User Account (Workspace).

It is carried out exclusively by API.

#### 7.5.2. Service description

The process of validating a Signature in a Signed Document or a Stamp in a Stamped Document is based on the following steps:

##### Step 1: Importing the signed or sealed document

The User, via his User Account, imports a Document that has already been signed or sealed in order to check its validity.

##### Step 2: Checking the signed or sealed document

For each Signature or Seal contained in a signed or sealed document, the Service checks that :

-The Certificate on which the signature is based was, at the time of the Signature, a Certificate compliant with the provisions of Regulation No. 910/2014/EU on electronic identification and trust services for electronic transactions within the internal market, known as the "eIDAS" Regulation;

- The certificate used was issued by a qualified trust service provider and was valid at the time of signing or sealing;

- The Signature or Seal validation data corresponds to the data communicated to the User;

- The unique set of data representing the signatory in the Certificate is correctly provided to the User;

- The Signature or Seal, if qualified, has been created by a qualified Electronic Signature or Seal creation device;

- The integrity of signed or sealed data has not been compromised;

### Step 3: Issuing and sending the Validation Report

Following the analysis of a signed or sealed Document, Universign issues a Validation Report which is then made available to the User once only via the API.

#### 7.5.3 Warranties

Subject to Users' compliance with the CGUET and applicable policies, Universign guarantees the enforceability, within the meaning of European regulations, of the content of Validation Reports created using the Service.

Universign also guarantees to provide a Service that complies with the Validation Policy.

#### 7.5.4. Warranty limits

Universign does not guarantee the suitability of the Service for the needs of the Customer and Users. It is up to them to verify this suitability, in particular by ensuring that the provisions of the Validation Policy meet their own requirements.

Use of the Service outside these guarantees is the sole responsibility of the Customer and Users.

#### 7.5.5. Validation report

After analysis of the signed or sealed Document that the User has wished to validate using the Service, a Validation Report is issued by Universign.

It contains the following information for each Signature / Seal present in the Document:

- the overall validation status of each signature/stamp;

- Signature/Stamp identifier (in the form of a hash) ;

- constraints applied during validation with a status (indicating the success of the verification or any errors encountered);

- the date and time of validation.

The Validation Report will be transmitted in the form of a file attesting to the authenticity of the data it contains and sealed by means of an Electronic Certificate in the name of Universign.

#### 7.5.6. Storage of Validation Reports

Universign stores only Validation Reports generated using the Service in such a way as to preserve their integrity.

Sealed or signed documents imported for Services purposes are deleted from the servers once the item analysis stage has been completed.

Universign reserves the right to store signed Validation Reports with a specialized subcontractor.

Validation reports and event logs are stored for seven (7) years from the date of issue, in accordance with applicable regulations.

However, it is specified that it is the responsibility of the Customer and Users to take all necessary measures to keep the Validation Report sent to them after the analysis, as it cannot be communicated at a later date by Universign.

#### 7.5.7. Obligations of Users

The User also undertakes to check that the signed or sealed Document submitted for validation as part of the Service is indeed the one sent to Universign.

The Service does not archive signed or sealed Documents submitted for validation, which remains the responsibility of Users.

#### 7.5.8. Limits of liability

Universign does not control the content of the signed or sealed Documents submitted for validation as part of the Service, and therefore cannot be held liable for the value and/or validity of the content of the Documents or for any defect therein.

Universign cannot be held responsible for inappropriate use of the Service.

#### 7.5.9. Policies and standards

Universign undertakes to comply with the policies and standards set out in the following table.

	<i>ETSI TS 119 441</i>	<b>PC Validation service</b>
<b>1.3.6.1.4.1.15819.5.7.1.1</b>	<i>ETSI EN 319 102-1</i>	Validation algorithm
	<i>ETSI TS 119 102-2</i>	Validation report format
1.3.6.1.4.1.15819.7.3.1	ETSI TS 119 44	DPV Signature Validation Service
1.3.6.1.4.1.15819.5.7.2.1		PV for qualified signatures and stamps
1.3.6.1.4.1.15819.5.7.2.2		PV for all types of signatures or stamps (qualified or not)

These policies are published on the website. They are audited by an accredited body in accordance with standard EN 319 403.

**Article 8 - SAFETY**

Universign undertakes to use its best efforts to secure the Service by deploying technical and organisational measures within the framework of the Services provided.

When accessing the Service, the Customer is expressly reminded that the Internet is not a secure network. Under these conditions, it is the Customer's responsibility to take all appropriate measures to protect their own data and/or software, in particular from possible misappropriation and contamination by any viruses circulating on the Internet or from the intrusion of a third party into their information system for any purpose whatsoever, and to check that files transmitted do not contain any computer viruses.

Universign declines all responsibility for the propagation of computer viruses, as well as for any consequences that may result from such viruses.

The Customer and Users must inform Universign of any failure or malfunction of the Service or of a User Account (Workspace) attached to a Workspace configured under the Customer's responsibility and used by Users.



If a security breach is detected, Universign will inform the Customer in accordance with the applicable legal provisions. It will inform them of any measures to be taken. The execution of these measures is the responsibility of the Customer and the Users of its Workspace.

Universign may take any emergency measures necessary for the security of a Workspace, and/or a User Account (Workspace) and/or the Service.

## **ARTICLE 9 - EFFECTIVE DATE - DURATION**

These GCUET apply from the moment a Customer creates a Workspace and from the moment a User Account (Workspace) is created for a User, for the entire duration of their use.

## **ARTICLE 10 - WARRANTIES**

### ***10.1. - Customer warranties***

The Customer guarantees Universign :

- That he/she holds the rights and authorizations required to create a Workspace and use the Service;
- Where applicable, if acting in a professional capacity, that it complies with the obligations incumbent on it with regard to its status as a trader and professional, in particular in terms of mandatory information;
- That it has collected and processes all the personal data it uses in the context of its Workspace in accordance with the regulations applicable to them regarding the protection of Personal Data and in all cases in accordance with the provisions of Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and any national laws to which it refers;
- That it is responsible for all use of the Services by Users in the context of its Workspace (including the User Account (Workspace)) and that, as such, it will implement all necessary control policies and procedures.

In the absence of these warranties, use of the Service by the Customer or any User is the sole responsibility of the Customer.

### ***10.2. - Universign guarantees***

Universign guarantees the confidentiality of the Documents transmitted to it under the terms and conditions described in the "Confidentiality" article.

### **10.3 - Warranty limits**

The Customer is informed that Universign does not verify in any way that the Service used corresponds to the Customer's needs and to the applicable regulations.

Universign excludes all warranties, in particular of latent defect, conformity to any need or use whatsoever, proper operation, or relating to the accuracy of the information provided, and declines all liability in the event of negligence on the part of the Customer or Users in the use of the Workspace or User Accounts (Workspace).

## **ARTICLE 11 - LIABILITY**

Universign's intervention is limited to a technical service by providing the Customer and Users with a Workspace, User Accounts (Workspace) and more generally software and technical tools enabling them to benefit from Services.

Universign undertakes to take all reasonable care in the execution of the Services in accordance with the best practices of its profession and in collaboration with the Customer and the Users operating under its responsibility, but shall only be bound by an obligation of means.

Universign shall in no event be liable for any damages other than those resulting directly and exclusively from a fault in the performance of the Service ordered, and in particular for any indirect or consequential damages such as loss of profits, sales, data or use thereof, or any other indirect or consequential damages arising from the use, delivery or performance of the Service.

Universign shall not be held liable in any way:

- In the event of illicit, misappropriated or non-conforming use of the Identifier of a User Account (Workspace) of the Workspace ;
- In the event of damage caused by the voluntary or involuntary disclosure to a third party of a User's Identifier;
- In the event of use of the Service that does not comply with the GTUET, and more generally with the policies applicable to the Services.

Unless otherwise agreed between the Parties, should Universign be held liable for any reason whatsoever and whatever the legal basis invoked or retained, all damages

combined and accumulated shall, by express agreement, be limited to the amount, exclusive of tax, paid by the Customer in return for the Service concerned during the 12 (twelve) months preceding the event giving rise to the damage.

This article will continue to have legal effect until the amount of compensation is determined.

## **ARTICLE 12 - INTELLECTUAL PROPERTY RIGHTS**

The Parties declare that they hold and retain free disposal of the intellectual property rights of the elements (brands, names, products, logos, etc.) intended to be used as part of the Service.

Any use or reproduction, in whole or in part, of these elements and/or the information they contain, by any process whatsoever, by either of the parties is strictly prohibited and constitutes an infringement liable to prosecution, with the exception of uses and reproductions previously and expressly authorized by each of the parties.

The CGUET do not imply any transfer of intellectual property rights held by the Customer, a User or Universign.

The Customer undertakes that Users of its Workspace will not download, reproduce, transmit, sell, distribute or exploit the content of the Service and the Website.

## **ARTICLE 13 - CONFIDENTIALITY**

Information transmitted or collected by Universign in the course of using the Service is considered confidential by nature and will not be communicated to any third party in any way unrelated to the provision of the Service, except in accordance with applicable legal and regulatory provisions.

This provision does not preclude judicial or administrative communications.

## **ARTICLE 14 - PERSONAL DATA**

Universign processes personal data in accordance with the **Personal Data Protection Policy**, which must be accepted by the Customer and Users prior to any use of the Services and which is available on the Website.

Data collected by Universign as part of the Service is kept for the time necessary to use the Workspace.

## **ARTICLE 15 - MISCELLANEOUS PROVISIONS**

**Force Majeure: In the event of the** occurrence of a case of force majeure, as usually understood by the jurisprudence of the French courts, Universign cannot be held responsible for a breach of any of its obligations hereunder, for the duration of such an impediment.

**Partial nullity:** In the event of difficulties of interpretation resulting from a contradiction between any of the titles appearing at the head of the clauses and any of the clauses, the titles will be declared non-existent.

Should any clause of these Customer Terms and Conditions be considered null and void, pursuant to a law or regulation or following a court decision, it shall be deemed unwritten and the other clauses shall remain in force.

**Independence of the parties:** Universign and the Customer acknowledge that they are each acting on their own behalf, independently of each other. The Contract does not constitute an association, a franchise, a partnership, an employee-employer relationship, or a mandate given by one of the Parties to the other. Neither Party may make any commitment in the name and on behalf of the other Party. In addition, each Party remains solely responsible for its acts, allegations, commitments, services, products and personnel.

**Commitments of the Parties :** The Customer is hereby informed that in the event that no specific commercial agreement has been signed between the Customer and Universign, only the CGUET and the other contractual documents described in the article "Contractual documents" are applicable to the performance of the Services.

It should be noted that all the CGUET and other applicable contractual documents are accessible on the Website in accordance with articles 1125 and 1127-1 of the French Civil Code.

Previous versions of the CGUET and other applicable contractual documents are also available on the Website. The Parties agree that such availability is for information purposes only and does not imply the applicability of such earlier versions.

It is understood that any new version of the CGUET cancels and replaces that previously agreed between the Parties having the same purpose and in progress.

**Notification:** Any complaint or notification from a Customer must be sent to Universign by post to its registered office at 7 rue du Faubourg Poissonnière 75009 Paris or via the forms available on the Website.

## **ARTICLE 16 - APPLICABLE LAW AND JURISDICTION**

These GCUET and the relationship between the Customer and Universign under them are governed by French law. This applies to both substantive and formal rules, notwithstanding the place of performance of substantial or ancillary obligations.

Only the French version of this document is binding, any translation being, by express agreement, for convenience only.

In the event of difficulties in the performance and/or interpretation of the contractual documents, and prior to bringing the matter before the competent courts, the parties agree to meet and use their best efforts to resolve the dispute.

Customers who must be considered as consumers within the meaning of the applicable law are informed that they may have recourse to a consumer mediator under the conditions set out in Title I of Book VI of the French Consumer Code.

In the absence of agreement between the Parties, each will regain its full freedom of action.

Unless otherwise agreed between the Parties, the Customer and Universign agree to submit to the exclusive jurisdiction of the competent courts of Paris to resolve any dispute relating to the validity, performance or interpretation of the GTUET.