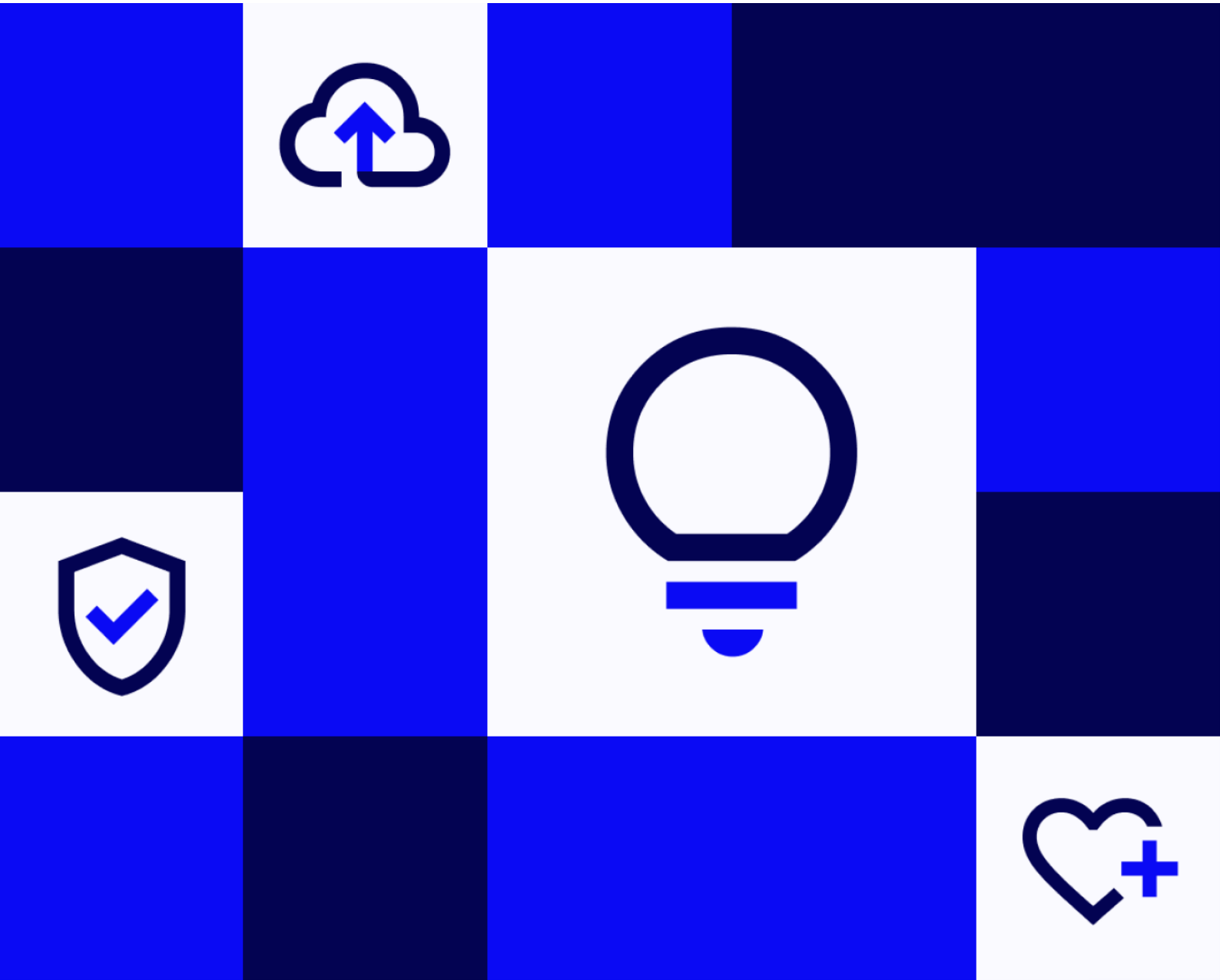
Terms and Conditions of Use

(Workspace)



These terms and conditions of use applicable to the Workspace (hereinafter "**Terms and Conditions of use of a Workspace**" or "**TCUW**") are intended to define the conditions of access and use of the Services proposed by Cryptolog International, Paris Commercial Registry No 439 129 164 (hereinafter "**Universign**") to its Clients who create and manage Workspaces under their responsibility, as well as to the Users invited to used them by a Client.

DEFINITIONS

Unless otherwise provided, terms beginning with a capital letter will have the meaning attributed in this article and may be used both in the singular and in the plural, according to context.

API: refers to the computer interface allowing access to the Service.

Certification Authority (CA): refers to the authority in charge of the creation, issuance, management and revocation of Certificates under the Certification Policy.

Preservation Authority (PA): refers to the authority in charge of the conservation of Electronic Signatures, working in particular through controls carried out on these elements and methods for the extension of Signature reliability beyond their period of technological validity.

Timestamping Authority (TA): refers to the authority in charge of the issuance of Timestamps in accordance with the Timestamping Policy.

Electronic Seal: refers to the procedure making it possible to guarantee the integrity of a sealed Document and to identify the origin of said Document through the Certificate used for its Sealing.

Client : refers to a natural or legal person who creates, configures or exclusively manages a Workspace as part of its professional activity in order to be able to use one or several Services and who (i) has accepted the Universign Terms and Conditions of Use - SaaS, or (ii) has signed a specific commercial agreement with Universign or one of its Partners to use one or several Services, as applicable.

User Account (personal account): refers to the computer resources attributed by Universign to a User wishing to use one or several specific Services. Each User Account (personal account) is attached to a User email address.

User Account (Workspace): refers to the computer resources attributed by Universign to a User wishing to use one or several specific Workspaces. Each User Account (Workspace) is attached to a unique User email address.

Personal Account Terms and Conditions of Use: refers to the terms and conditions of use applicable to Users wishing to benefit from specific Services. They are available on the Website.

Conservation: refers to the associated Service consisting of the implementation of procedures and technologies making it possible to extend the reliability of Electronic Signatures for a fixed period.

Timestamp: refers to a structure which links a Document to a specific moment, therefore offering proof that it existed at that time.

Electronic Document or Document: refers to the set of structured data that may be electronically processed by the Service.

Documentation: refers to the functional and technical documentation provided by Universign as part of the Services' use.

Registration File: refers to the file upon whose basis the Certificate request is made containing the information and supporting documents required by the Certification Policy.

Workspace: refers to the computer resources allocated to the Client by Universign and which allow it to invite Users to use the Services.

Timestamping: refers to a process making it possible to prove that a Document existed at a given moment, through the use of Timestamps.

Username: refers to the specific characters with which each User logs in to the Service.

Updates: refers to the successive versions of the Platform including technical improvements and/or features, provided by Universign. Updates include all modifications brought to the Platform to comply with regulatory changes and changes affecting the operating environment.

Delegated Registration Operator or DRO: refers to a User who carries out the registration operations for Certificate holders on behalf and under the instructions of Universign and who, as a result, is responsible for the verification of the Certificate holder's identity in its presence (with a face-to-face meeting) and for the constitution of its Registration File.

Partner: refers to a natural or legal person who integrates or markets one or several Universign Services with the solutions it publishes, in order to make these available to a Client.

Platform: refers to the technical infrastructure composed of all its materials, software packages, operating system, Updates, database, and environment managed by Universign or its subcontractors, on which the Software Package will be used. This allows for the provision of the Software Package in SaaS mode. It is remotely available directly via the internet network on the Website or through a smartphone or touchscreen tablet.

Certification Policy (CP): refers to the set of rules, identified by a number (OID), defining the requirements with which a CA complies in the implementation and provision of its services.

Preservation Policy (PP): refers to all the rules to which the PA complies for the implementation of the Conservation Service.

Personal-Data Protection Policy or PDPP: refers to the document presenting the information regarding personal

data processed by Universign as part of the Services, the purposes and basis of said processing, the sharing of this data with third parties, as well as the rights applicable to the Users having transmitted said data.

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

Timestamping Policy (TP): refers to all the rules to which the TA complies for the implementation of the Timestamping Service.

Holder: refers to the natural or legal person identified in the Certificate, having control over the private key corresponding to the public key.

Software Package: refers to the set of programs, procedures and rules, as well as the Documentation relating to the operation of an information-processing system. The Software Package is developed by Universign to allow the provision of Services in SaaS mode.

Validation Report: refers to the document issued by Universign following analysis of the Signature or Seal 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 through a connection to the shared Platform hosted on the Universign's servers or those of its subcontractors.

Electronic Sealing or Sealing: refers to a procedure making it possible to guarantee the integrity of a sealed Document and to identify the origin of said Document through the Certificate used for its sealing.

Service(s): refers to the set of services and software solutions in SaaS mode that Universign undertakes to provide to the Client.

Signatory: refers to the natural person hoping to conclude or having concluded a Transaction with the User through the Service.

Electronic Signature or Signature: refers to a procedure making it possible to guarantee the integrity of the signed Document and to demonstrate the consent of the Signatory it identifies.

Website: refers to the website www.universign.com.

Storage: refers to the service associated with the Universign Electronic-Signature Service consisting of the option to store Documents signed via the Service on the Platform.

Universign Support: refers to the Universign web assistance available via the URL https://help.universign.com/.

Transaction: refers to the process between the Client and which may include a third party, during which an Electronic Document proposed by the Client is signed or timestamped via the Service.

User: refers to a natural person who is a member of at least one Workspace and who has, in this context, an account with specific obligations and rights according to its role to be able to use the Services for professional purposes. The User using a Service within a Workspace acts under the contractual liability of the Client having created said User.

ARTICLE 1 – PURPOSE

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

ARTICLE 2 – CONTRACTUAL DOCUMENTS

The contract between Universign and the Client is made up of the following contractual documents presented in decreasing hierarchical order of legal value:

- Policies related to the subscribed Service, which are published on the website;
- The Universign Terms and Conditions of Sale or the applicable specific commercial agreement, as appropriate
- The PDPP
- These TCUW;
- The TCUPA, if applicable;

In case of contradiction between one or several stipulations appearing in the documents indicated above, the higher ranking document will prevail.

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

The TCUW are permanently accessible on the Website.

ARTICLE 3 – ACCEPTANCE

Before any use of the Service, the Client acknowledges having read the TCUW and accepts them without reserve.

The Client's acceptance is indicated by clicking the checkbox on the Website during the creation of a Workspace.

It therefore recognizes that its commitment does not require a handwritten or electronic signature.

ARTICLE 4 – WORKSPACE

4.1. – Creation of a Workspace

Access and use of the Service requires the creation of a Workspace.

The Workspace is created by the Client, who may configure one or several and designate one or several Users, within the limit of rights subscribed to.

Each User will have more or less extensive rights according to their profile.

By default, the Client has a Workspace owner profile with the broadest rights.

The Client can create one or several Workspaces to benefit from a Service, as long as it has:

- Suitable computer equipment to access the Service;
- A valid and personal email address (for which it controls access)

4.2. – Access to the Workspace

To access the Workspace, the Client must authenticate itself using the Username it has freely determined at the time of the creation of its first Workspace.

The Client's Username is strictly personal. It must meet the security criteria established by Universign and must not, under any circumstances, be communicated to third parties.

It is expressly recalled that Universign will never ask the Client, for any reason, to communicate its Username, and that any such request must be considered a fraudulent request.

The Client is wholly responsible for the preservation and use of its username. It must take all necessary measures to prevent unauthorized or fraudulent use of the Workspace.

If the Client notes or suspects unauthorized or fraudulent use of its username or those of its Workspace's Users, it must immediately alert Universign via the Universign Support service.

As of receipt of this notification, Universign will proceed to disable the User Account (Workspace) in question within a reasonable time period.

Article 4.3. – Invitation of Users to a Workspace

The Client may invite one or several Users to the Workspace for which it is owner.

A User's access to a Workspace requires their prior acceptance of the TCUW.

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

Article 4.4. – Use of the Workspace

The Client undertakes to ensure that the Users of its Workspace provide Universign with exact information for the use of the Service. The Client ensures that Users refrain from any abnormal, abusive, or fraudulent use of the Service. In particular, it undertakes to ensure that Users access the Service via API in a way compliant with the Documentation.

In general, the Client undertakes to ensures that Users refrain from any activity implemented through the Service which would not comply with the laws and regulations applicable thereto.

Non-respect of the conditions of use of a Service from a Workspace will engage the exclusive liability of the Client, without prejudice to the immediate deactivation of a User Account (Workspace) or any liability action that Universign reserves the right to exercise.

Article 4.5. – Closure of a Workspace

The Client may decide to close the Workspace it has created using the Universign solution.

ARTICLE 5 – USER ACCOUNT (WORKSPACE)

5.1. – Creation of a User Account (Workspace)

The Workspace is created by the Client, who designate one or several Users, within the limit of rights subscribed to.

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

- the User is a Client and has created a Workspace
- the User has been invited by a Client to the Workspace it has configured.

Each User will have more or less extensive rights according to the Profile it has been attributed by the Client.

The User may create a User Account (Workspace) to use a Service, as long as it has:

- Suitable computer equipment to access the Service;
- A valid and personal email address (for which it controls access)

5.2. – Access to the User Account (Workspace)

To access the User Account (Workspace), the Client must authenticate itself using the Username it has freely determined at the time of the creation of its User Account (Workspace).

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

It is expressly recalled that Universign will never ask the User, for any reason, to communicate its Username, and that any such request must be considered a fraudulent request.

The User is wholly responsible for the preservation and use of its username. It must take all necessary measures to prevent unauthorized or fraudulent use of its User Account (Workspace).

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

As of receipt of this notification, Universign will proceed to disable the User Account (Workspace) in question within a reasonable time period.

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

Article 5.3. – Closure of a User Account (Workspace)

The closure of a User Account (Workspace) may be carried out by the Client or any User having the appropriate functional rights.

ARTICLE 6 – SERVICES PROVIDED

6.1. – Delivery and evolution of the Service

The Services are delivered in SaaS mode (Software as a Service). They are subject to regular Updates intended to improve their quality and/or the existing features for all Users.

Universign reserves the right to complete or modify the Service, at any time, according to technical evolutions and to inform Users by any means.

These Updates will be considered to form part of the Service and will be subject to the terms hereof.

Users are recommended to regularly consult the Website, where information regarding new evolutions will be communicated.

Universign reserves the right to temporarily limit access to the Service, without notice nor compensation, in particular to carry out Updates, maintenance operators, modifications or changes to operational methods, or accessibility hours, without this list being understood as exhaustive.
Universign is not responsible for damages of any nature that may result from these changes and/or a temporary unavailability of the Website, the API or the Service.

6.2. – Service Quality

Universign endeavors to provide a Service compliant with the policies in force, available on the Website.

Due to the nature and complexity of the internet and, in particular, its technical performances and response times for the consultation, querying, or transfer of data, Universign cannot therefore ensure absolute availability of the Website, the API and, more generally, the Service.

Universign cannot be held liable for the proper functioning of the User's computer or telephonic equipment, nor its access to the internet or to a mobile-telephony network.

The User remains responsible for the telecommunication costs billed by its internet-connection operator during the Service's use.

ARTICLE 7 - SPECIFIC CONDITIONS OF USE OF THE SERVICES

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

7.1. – Timestamping service

The Service allows for the timestamping of Documents via Timestamps issued according to the Timestamping Policy which more precisely describes the Service's implementation and organization.

7.1.1. Access to the Service

The Signatory may benefit from the Service offered as long as they have:

- A User Account (Workspace).

Use of the Service through API requires the configuration of the User's information system according to the instructions provided in the Documentation.

7.1.2. Use of the Service

The User delivers the Document to be timestamped to the Service, via the Universign API, in accordance with the Documentation.

In response to the User's request, the Service delivers a Timestamp whose constituent elements are described in the Timestamping Policy.

7.1.3. Service description

The Service must not be used to establish proof that an email has been sent to or received by a recipient. The Service does not constitute a registered electronic-delivery service. The Service must not be used for the purpose of identifying the author or origin of the Document.

7.1.4. Guarantees and limitations of guarantees

Subject to the Client and User's respect for the applicable TCUW and applicable policies, Universign ensures the enforceability of Timestamps created through the service, within the meaning of European regulations.

Timestamping carried out via the Service benefits from a presumption of accuracy of the date and time contained in the Timestamp and of the integrity of the Document to which said Timestamp relates.

The Timestamping Service is synchronized with universal coordinated time to ensure that Timestamps have a precision of one (1) second.

In case of any event affecting the Service's security and which may impact Timestamps, appropriate information will be provided to Users via the Website.

Universign does not guarantee the Service's suitability for the Client and User's needs. It is the User's responsibly to verify this suitability, in particular by ensuring that the provisions of the Timestamping Policy meet its own requirements.

7.1.5. User's obligation

The User undertakes to verify the validity of Timestamps as of their reception according to the verification procedure described in the Timestamping Policy.

The information necessary for the performance of the Timestamp verification procedure described in the Timestamping Policy is available on the Website.

Outside of the cases provided for by the Timestamping Policy, Timestamps may be verified for five (5) years as of their issuance.

The User also undertakes to verify that the Timestamped document is indeed that transmitted to Universign for Timestamping.

The archiving of Timestamps falls under the exclusive responsibility of the User.

7.1.6. Data retention

In accordance with the Timestamping Policy and applicable regulations, Universign retains event logs regarding the Service's functioning for a period of six (6) years.

7.1.7. Policies and standards

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

1.3.6.1.4.1.15819.5.1.1	ETSI EN 319 411-1	Timestamping Authority CP
1.3.6.1.4.1.15819.5.2.2	ETSI EN 319 421	Timestamping Policy

These Policies are published on the Website. They are audited according to the EN 319 403 standard by an accredited body.

7.2. – Electronic-Seal Service

The Service allows the implementation of Electronic Seals, whose legal effects are recognized by applicable regulations across the European Union.

7.2.1. – Access to the Service

Access to the Service requires:

- A User Account (Personal Account);
- A User Account (Workspace)
- A legal-person Certificate associated with cryptographic keys compliant with one of the Certification Policies mentioned herein.

Access to the Service through API requires the configuration of the User's information system according to the instructions provided in the Documentation.

The Documentation is provided by Universign upon the User's request, after the creation of its User Account (Workspace).

7.2.2. – Use of the Service

The User delivers 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 delivers the Document to which an Electronic Seal has been affixed.

7.2.3 – Limitations of use

The Service makes it possible to attach an Electronic Seal to a Document. It must not be used to establish proof of consent from the Holder 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. Categories of Electronic Seals

7.2.4.1. Level-1 Electronic Seal

Category-1 Electronic Seals are created via Certificates compliant with the requirements of the ETSI EN 319 411-1 standard, which provides in particular the possibility of remote verification of the Holder's identification data.

7.2.4.2 Level-2 Electronic Seal

Category-2 Electronic Seals are created via Qualified Certificates compliant with the requirements of the ETSI EN 319 411-2 standard, which provides in particular the verification of Holder supporting documents in the presence of its expressly authorized representative.

7.2.4.3 Level-3 Electronic Seal

Qualified category-3 Electronic Seals are created via Qualified Certificates compliant with the requirements of the ETSI EN 319 411-2 standard, which provides in particular the verification of Holder supporting documents in the presence of its expressly authorized representative.

7.2.5. Guarantees and limitations of guarantees

Subject to the Client and User's respect for the applicable TCUW and applicable policies, Universign ensures the enforceability of Electronic Seals created through the service, within the meaning of European regulations.

Universign does not guarantee the Service's suitability for the User's needs. It is the User's responsibly to verify this

suitability, in particular by ensuring that the provisions of the Certification Policy meet its own requirements.

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

7.2.6. – User's obligations

The User also undertakes to verify that the sealed Document is indeed that transmitted to Universign for the creation of an Electronic Seal.

The archiving of sealed Documents falls under the exclusive responsibility of the User.

7.2.7. - Data retention

Universign retains event logs regarding the Service's functioning for a period of fifteen (15) years from the sealing date.

7.2.8. Policies and standards

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

1.3.6.1.4.1.15819.5.1.3.4	ETSI EN 319 411-1	CP for legal-person certificates, LCP level
1.3.6.1.4.1.15819.5.1.3.5	ETSI EN 319 411-2	CP for legal-person certificates, QCP-I level

These policies are published on the Website. They are audited according to the EN 319 403 standard by an accredited body.

7.3. – Electronic-Signature Transaction management service

The Transaction-management Service offers Users access to an Electronic-Signature creation solution allowing them to collect from one or several Signatories.

7.3.1. Access to the Service

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

This may be done via API or via the Website.

7.3.2. Service description

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

The process for the Electronic-Signature of Documents is based on the following steps:

Step 1: Provision of the Document

A User, via a Workspace, makes available the Document to be signed and, if applicable, to read, for the Signatory.

Step 2: Invitation to sign

The User fills in the data regarding the Signatory required by the Service.

Step 3: Access to the signed Document

Access to the original signed Document may be made via the Client's Workspace.

7.3.3. Limitations of use

The User undertakes not the misuse the Service's features or the Signatory authentication means, in particular by filling in information regarding the Signatory that it knows to be erroneous or by not permitting the Signatory to properly view the Document intended to be signed, or by entering the confidential code sent to the Signatory itself.

Any use of the Service not compliant herewith may entail the non-enforceability of the Electronic Signature and/or the nullity of the deed to which it is attached.

7.3.4. Levels of Electronic Signatures

The Service allows the implementation of three levels of Electronic Signature, whose legal effects are recognized by applicable regulations across the European Union.

7.3.4.1. Level-1 Electronic Signature

As part of the implementation of the level-1 Signature, Universign cannot guarantee the identity of the Signatory, nor their authorizations. The Client will be responsible for identifying the Signatory via its own organizational and technical processes, which it implements under its exclusive liability.

Universign authenticates the Signatory via the Signatory's telephone number as declared to Universign (by the Signatory themselves or by the Client), as applicable.

The Level-1 Electronic Signature does not require the creation of a User Account (personal account) by the Signatory.

In the context of this Signature's use, Universign cannot guarantee the Signatory's identity – the only elements provided being those communicated by the User.

The Identification data appearing on the Electronic Signature is that 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 verification of Signatory Identification is carried out remotely via a digital copy of their identity document delivered to Universign.

Universign authenticates the Signatory via the Signatory's telephone number as declared to Universign (by the Signatory themselves or by a User), as applicable.

In the context of this Signature's use, Universign cannot guarantee the Signatory's identity. As such, the Client is responsible for implementing organization or technical processes to ensure that Users of its Workspace verify the Signatory's identity via their own means and under their exclusive liability.

Universign verifies the consistency between the identification declared and the identity document for which a copy has been delivered thereto.
The level-2 Electronic Signature is made via Certificates compliant with the requirements of the ETSI EN 319 411-1 standard.

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

7.3.4.3. Level-3 Electronic Signature

As part of the implementation of the level-3 Electronic Signature, Universign or a DRO verifies the identity of the Signatory in person and via an identity document.

Universign authenticates the Signatory via the Signatory's telephone number as declared to Universign (by the Signatory themselves or by the User), as applicable.

The level-3 Electronic Signature is made via qualified Certificates compliant with the requirements of the ETSI EN 319 411-2 standard.

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

7.3.4. Guarantees and limitations of guarantees

Within the context of the implementation of the level-3 Electronic Signature, Universign guarantees the use of a qualified Certificate whose issuance is subject to the verification of the Signatory's identity via appropriate means, compliant with French law.

Subject to the Users' respect for the TCUW and applicable policies, Universign ensures the enforceability of Electronic Signatures created through the service, within the meaning of European regulations.

In no case will Universign verify that the Service corresponds to the legal regimes applicable to the Documents. Consequently, the provision of the Service does not exempt Users from the responsibility to analyze and verify applicable legal or regulatory requirements.

7.3.5. Document storage

Unless otherwise notified by the Client, Universign stores the Documents signed via the Service so as to preserve their integrity. Storage allows the Client and the Users of these Workspaces to consult signed Documents online, and ensures their Conservation, return. and/or destruction.

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

Universign reserves the right to store signed Documents with a specialist subcontractor.
If Storage is carried out by Universign and unless otherwise agreed between Universign and the Client, the Documents are stored from their filing until the occurrence of one of the following events:

- Fifteen (15) years after the date of the Document's filing;
- The manual deletion of a Workspace Document by a User
- The closure of the Workspace;
- Two (2) months after the end of a Contract, unless it is extended by a period of reversibility;

It is the Client's responsibility to take any provisions so as to conserve Documents no longer or not stored in a Workspace in a way that is durable and ensures their integrity.

7.3.6 Users' obligations

Each User undertakes to:

- the content of the Documents is legal and not to allow the performance of illegal acts or those contrary to applicable laws and regulations;
- the content of the Documents does not infringe on the privacy of persons and/or the provisions relating to the protection of personal data and/or competition law, and/or consumer law.

The use of the Service outside of these guarantees engages the Client's exclusive liability.

7.3.7 Client's obligations

The Client undertakes:

-If applicable, if it acts as a trader or professional, to respect the obligations imposed thereupon with regard to its status, particularly in terms of compulsory mentions and the transmission of signed Documents;
-to implement all technical, legal or organizational measures allowing it to ensure the proper use of Services by the Users of its Workspaces

7.3.8. Limitation of liability

Universign does not control the content of Documents and as such its liability may not be engaged with regard to the value and/or validity of the content of Documents, or lack thereof.

Universign's liability may not be engaged for consequences of decisions that may have been taken or actions that may be undertaken based on these Documents (whether signed or not).

Universign cannot be held liable 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 mentioned in the following table.

1.3.6.1.4.1.15819.5.1.3.3	ETSI EN 319 411-1	CP for natural-person certificates, LCP level
1.3.6.1.4.1.15819.5.1.3.1	E T S I E N 3 1 9 - 4 1 1 - 2	CP for natural-person certificates, QCP-l level

These policies are published on the publication Site. They are audited according to the EN 319 403 standard by an accredited body.

7.3.10. Evidence file

For signatures, Universign will provide Users with the Data extracted from its event log contributing to establishing proof of the constituent operations of an Electronic Signature, subject to the presentation of the appropriate supporting document, in accordance with the existing procedure that may be communicated to Users upon simple request addressed to Universign Support.

The Client authorizes Universign to communicate the evidence file relating to a signed Document to any Workspace User.

This data will be transmitted in the form of a file attesting to the authenticity of said data and stamped via an Electronic Certificate in Universign's name.

Legal Evidence Files are stored for a period of 15 years as of the Document's Signature by all Signatories.

7.4. – Service de Conservation

The Conservation Service makes it possible to extend the reliability of Documents forming the subject of Electronic Signature beyond their period of technological validity, in accordance with the Preservation Policy which more precisely describes the Service's implementation and organization.

7.4.1. Access to the Service

Access to the Service is an option included in the Electronic-Signature service provided by Universign.

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

By default, the Service is provided to all Clients storing electronically signed Documents with a Universign solution. It may be disabled upon the Client's request.

7.4.2. Use of the Service

When electronically signed Documents are stored by Universign, the latter carries out processing via its solution allowing the reliability of the Signatures said Documents contain to be extended beyond their period of technological validity.

The Service therefore includes all elements described in the Preservation Policy within the electronically signed Document.

7.4.3. Limitations of Use

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

7.4.4. Guarantees and limitations of guarantees

Furthermore, Universign guarantees the provision of a Service compliant with the Preservation Policy.

Universign does not guarantee the Service's suitability for the Client's needs. It is the Client's responsibly to verify this suitability, in particular by ensuring that the Services, as well as the provisions of the Preservation Policy, meet its own requirements.

The use of the Service outside of these guarantees engages the Client's exclusive liability.

7.4.5. Document Storage

It is the User's responsibility to take any provisions to store electronically signed 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 Preservation Service for a period of fifteen (15) years.

7.4.7. Limitation of liability

Universign does not control the content of Documents processed as part of the Services, and as such its liability may not be engaged with regard to the value and/or validity of the content of said Documents, or lack thereof.

Universign's liability may not be engaged for consequences of decisions that may have been taken or actions that may be undertaken based on these Documents for which reliability has been extended beyond the period of technological validity.

7.4.8. Policies and standards

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

1.3.6.1.4.1.15819.5.8.1	ETSI TS 119 511	PP for conservation via extension of signed documents
1.3.6.1.4.1.15819.7.4.1	ETSI TS 119 511	PPD for conservation via extension 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		Conservation-Evidence Policies

These policies are published on the publication Site. They are audited according to the EN 319 403 standard by an accredited body.

7.5. – Electronic-Signature and Seal Validation Service

The Signature and Seal validation Service allows a User to validate a Signature and Seal previously carried out.

7.5.1. Access to the Service

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

This is carried out exclusively via API.

7.5.2. Service description

The validation process for a Signature in a signed Document or a Seal in a sealed Document is based on the following steps:

Step 1: Import of the signed or sealed Document

Via its User Account, the User imports a previously signed or sealed Document in order to verify its validity.

Step 2: Verification of the signed or sealed Document

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

-The Certificate upon which the signature is based was, at the time of the Signature, a Certificate compliant with the provisions of Regulation 910/2014/EU on electronic identification and trust services for electronic services within the internal market, known as the "eIDAS" regulation;
- The Certificate used was issued by a qualified trust-services provider and was validated at the time of the Signature or Sealing;
- The Signature or Seal's validation data correspond 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, were created via a device for the creation of qualified Electronic Signatures or Seals;
- The integrity of signed or sealed data has not been compromised;

Step 3: Issuance and delivery of the Validation Report

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

7.5.3. Guarantees

Subject to the Users' respect for the TCUW and applicable policies, Universign ensures the enforceability of the content of Validation Reports created through the service, within the meaning of European regulations.

Furthermore, Universign guarantees the provision of a Service compliant with the Validation Policy.

7.5.4. Limitations of guarantees

Universign does not guarantee the Service's suitability for the Client and User's needs. As such, it is their responsibly to verify this suitability, in particular by ensuring that the provisions of the Validation Policy meet their own requirements.

The use of the Service outside of these guarantees engages the Client's and the Users' exclusive liability.

7.5.5. Validation Report

After analysis of the signed or sealed Document that the User wishes to validate via the Service, a Validation Report is issued by Universign.
For each Signature/Seal present in the Document, it contains the following information:

- the overall validation status of each Signature/Seal;
- the Signature/Seal's ID (in the form of a hash);
- the constraints applied during validation with a status (indicating the success of the verification carried out 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 stamped via an Electronic Certificate in Universign's name.

7.5.6. Storage of Validation Reports

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

Sealed or signed Documents imported for the needs of the Services are deleted from the servers once the analysis step has been completed.

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

The Validation Reports and the event logs are stored for seven (7) years after their issuance in accordance with application regulations.

However, it is specified that it is the Client and User's responsibility to take any provisions to retain the Validation

Report transmitted thereto after analysis, as this cannot be subsequently re-communicated by Universign.

7.5.7. Users' obligations

The User also undertakes to verify that the signed or sealed Document subject to validation as part of this Service is indeed that transmitted to Universign.
The Service will carry out not archiving of signed or sealed Documents subject to validation, with this remaining the responsibility of Users.

7.5.8. Limitations of liability

Universign does not control the content of Documents signed or sealed subject to validation as part of the Service, and as such its liability may not be engaged with regard to the value and/or validity of the content of the Documents, or lack thereof.

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

7.5.9. Policies and standards

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

1.3.6.1.4.1.15819.5.7.1.1	*ETSI TS 119 441*	CP Validation service
	ETSI EN 319 102-1	Validation algorithm
	ETSI TS 119 102-2	Format of validation report
1.3.6.1.4.1.15819.7.3.1	ETSI TS 119 44	VPD Signature-validation service
1.3.6.1.4.1.15819.5.7.2.1		VP for qualified signatures and seals
1.3.6.1.4.1.15819.5.7.2.2		VP for all types of signatures or seals (qualified or not)

These policies are published on the Website. They are audited according to the EN 319 403 standard by an accredited body.

Article 8 – SECURITY

Universign undertakes to ensure its best efforts to secure the Service, by implementing technical and organizational measures as part of the Services provided.

As part of its access to the Service, the Client is expressly reminded that the internet is not a secure network. Under these conditions, the Client is responsible for taking all appropriate measures to protect its own data and/or software from, for example, any alteration and contamination by viruses circulating on the internet and from third-party intrusion into its information system for any purpose, and to verify that the transmitted files contain no computer viruses.

Universign declines all liability with regard to the spread of computer viruses, as well as all consequences that may result from said viruses.

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

If a security fault is detected, Universign will inform the Client in compliance with the applicable legal provisions. It will indicate any measures to be taken. The Client and the Users of its Workspace are responsible for the performance of these measures.

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

ARTICLE 9 – ENTRY INTO FORCE - TERM

These TCUW are applicable as of the creation of a Workspace by a Client and the creation of a User Account (Workspace) with regard to a User, for the entire duration of their use.

ARTICLE 10 – GUARANTEES

10.1. – Client's guarantees

The Client guarantees to Universign:

- That it is the holder of the rights and powers necessary for the creation of a Workspace and the use of the Service;
- If applicable, if it acts as a professional, that it respects the obligations imposed thereupon with regard to its status as a trader or professional, particularly in terms of compulsory mentions;
- That it has collected and processed the personal data it uses as part of its Workspace in accordance with the regulations applicable thereto with regard to Personal Data and, in any case, in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and any national law to which it refers;
- That it is responsible for any use of the Services by Users as part of its Workspace (including User Accounts (Workspace)) and that, as such, it will implement all necessary policies and control procedures.

In the absence of these guarantees, the use of the Service by the Client or any User engages the Client's exclusive liability.

10.2. – Universign's guarantees

Universign guarantees the confidentiality of the Documents transmitted to its hereunder, under the conditions described in the article "Confidentiality".

10.3. – Limitations of guarantees

The Client is informed that Universign will, in no case, verify that the Service uses corresponds to its needs and to the regulations applicable thereto.

Universign excludes any guarantee, in particular for hidden defect, conformity to any need or use, proper functioning, or relating to the accuracy of information provided, and declines any liability in case of negligence by the Client or Users in the Use of the Workspace or User Accounts (Workspace).

ARTICLE 11 – LIABILITY

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

Universign undertakes to provide all reasonable care in the performance of the Services, in accordance with best practices and in collaboration with the Client and Users acting under its liability, but may only be held to an obligation of means.

Universign may, in no case, be held liable for damages other than those directly and exclusively resulting from a fault in the performance of the ordered Service and, in particular, for any indirect or immaterial damage such as loss of profits, turnover, data or use thereof, or any other indirect or immaterial damage arising from the use, delivery, or performance of the Service.

Universign's liability may not be sought:

- In case of misuse or illegal or non-compliant use of the Username for a Workspace User Account (Workspace);
- In case of damages caused by the voluntary or involuntary disclosure of a User's Username to a third party;
- In case of use of the Service which does not comply with the TCUW and, more generally, with the policies applicable to the Services.

Unless otherwise agreed between the Parties, should Universign's liability be retained, for any reason and regardless of the legal grounds invoked or held, all damages combined and cumulated will be, by express agreement, limited to the amount excluding tax paid by the Client for the Service in question over the 12 (twelve) months prior to the damages' generating fact.

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

ARTICLE 12 – INTELLECTUAL PROPERTY

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

Any total or partial use or reproduction of these elements and/or the information they contain, by any procedure and by either Party, is strictly prohibited and constitutes an infringement liable to prosecution, with the exception of the uses and reproduction previously and expressly authorized by each of the Parties.

The TCUW do not imply any transfer of intellectual-property rights held by the Client, a User or Universign.

The Client undertakes to ensure that the Users of its Workspace do not download, reproduce, transmit, sell, distribute, or market the content of the Service and the Website.

ARTICLE 13 – CONFIDENTIALITY

The information transmitted or collected by Universign as part of the Service's use is considered confidential by nature and will not be subject to any external communication not related to the Service's provision, excluding any exceptions related to applicable legal and regulatory provisions.

This provision does not preclude communications ordered by a legal or administrative authority.

ARTICLE 14 – PERSONAL DATA

Universign carries out personal-data processing in accordance with the Personal-Data Protection Policy which must be previously accepted by the Client and the Users before any use of the Services, and which is available on the Website.

The data collected by Universign as part of the Service is retained for the time necessary for the Workspace's use.

ARTICLE 15 – MISCELLANEOUS PROVISIONS

Force Majeure: Should a case of force majeure arise, in the sense normally understood by the case law of French courts, Universign may not be held liable for a breach of one of its obligations hereunder, for the duration of such an impediment.

Partial nullity: In case of difficulties in interpretation resulting from a contradiction between any of the titles indicated at the top of the clauses and any of the clauses, the titles will be declared non-existent.

Should any clause of these Client Terms and Conditions be considered null and void, in application of a law or regulation or following a judicial decision, it will be deemed to have not been written and the other clauses will remain in force.

Parties' independence: Universign and the Client acknowledge that each Party acts on its own behalf, independently of the other. The Contract does not constitute an association, franchise, partnership, employee-employer relationship nor a mandate given by one of the Parties to the other Party. Neither Party may enter into an agreement in the name of and on behalf of the other Party. Furthermore, each of the Parties remains solely liable for its actions, allegations, commitments, services, products, and staff.

Parties' commitments: The Client is informed that, if no specific commercial agreement has been signed between the Client and Universign, only the TCUW and other contractual documents described in the article "Contractual documents" will be applicable to the Services' performance.

It should be noted that all TCUW and other applicable contractual documents may be accessed on the Website in accordance with articles 1125 and 1127-1 of the Civil Code.

Previous versions of the TCUW and other applicable contractual documents are also available on the Website. The Parties agree that these are only provided for informative reasons and do not imply the applicability of previous versions.

It is understood that any new version of the TCUW cancels and replaces that previously accepted by the Parties with the same subject and currently underway.

Notification: Any Client complaint or notification must be delivered to Universign by postal mail at its registered office at 7 Rue de Faubourg Poissonnière - 75009 Paris or via the forms available on the Website.

ARTICLE 16 – APPLICABLE LAW AND JURISDICTION

These TCUW, as well as the relationship between the Client and Universign thereunder, are governed by French Law. This applies both to substantive and formal rules, regardless of where substantial or ancillary obligations are performed.

Only the French version of this document is enforceable, with all translations made being, by express agreement, made only for simple convenience.

In case of difficulties in the performance and/or interpretation of the contractual documents and prior to the referral to the competent courts, the Parties agree to come together and implement their best efforts to resolve their dispute. Clients, who must be considered consumers under applicable law, are informed that they have the right to turn to a consumer mediator under the conditions provided in section I of book VI of the French Consumer Code.

In the event of an absence of agreement between the Parties, each Party will regain full freedom to pursue legal action.

Unless otherwise agreed by the Parties, the Client and Universign accept to submit themselves to the exclusive jurisdiction of the competence courts of Paris, with a view to resolving any dispute regarding the validity, performance or interpretation of the TCUW.