universign

Terms and Conditions of Use

(Signatory, Reviewer)

The Signatory Terms and Conditions of Use (hereinafter the "**Terms and Conditions of Use (Signatory, Reviewer)**" or "**TCUSR**") are intended to define the legal conditions applicable to signatories wishing to sign Documents from the Platform made available by Cryptolog International, Paris Commercial Registry No 439 129 164 (hereinafter "**Universign**"), via its Clients or Partners.

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.

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

"**Certificate**" refers to the electronic file issued by the Certification Authority including the identification elements of its Holder and a cryptographic key facilitating the verification of the Electronic Signature or electronic seal for which it is used.

Qualified Certificate: refers to a Certificate meeting the requirements of article 28 or 38 of European Regulation 910/2014 of 23 July 2014.

Electronic Seal or 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.

Collection: refers to the Client's action consisting of sending one or several documents on the Universign platform so that they may be signed by one or several Signatories.

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.

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 the period in which signed Documents are stored by Universign.

Document: refers to a set of structured electronic data that may be processed by the Service.

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

Personal Data refers to any information regarding an identified or identifiable person, whether directly or indirectly.

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

Workspace: refers to the computer resources allocated to the Client by Universign and which allow it to invite Signatories to sign a Document.

Delegated Registration Operator or DRO: refers to a natural person who carries out the registration operations for Certificate holders on behalf and under the instructions of Universign and who, as a result, proceeds to the verification of the Certificate Holder's identity in its presence (therefore via a face-to-face meeting) and 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.

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.

Holder: refers to the natural person identified in the Certificate, having control over the private key corresponding to the cryptographic key appearing in the Certificate.

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.

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.

Service(s): refers, within this contract, to the Universign Electronic-Signature service provided to the Signatory via a Client.

Signatory: refers to a natural person using the Platform to sign a Document.

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 Universign Storage Service for the Signatory's signed Documents.

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

Personal-Data Processing refers to an operation or set of operations regarding Personal Data, no matter the procedure used.

Reviewer: refers to a natural person using the Platform to review a Document before it is presented for signature by a Signatory.

ARTICLE 1 – PURPOSE

These Terms and Conditions of Use for Signatories define the conditions applicable to a Signatory using the Electronic-Signature Service.

ARTICLE 2 – CONTRACTUAL DOCUMENTS

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

- Policies related to the Service published on the website;
- These TCUSR;

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 Signatory Terms and Conditions of Use at any time and without notice.

The applicable Signatory Terms and Conditions of Use are permanently accessible on the Website, and in a format allowing their printing and/or download.

ARTICLE 3 – ACCEPTANCE

Before any use of the Service, the Signatory acknowledges:

- Having read the applicable TCUSR;
- That they have the legal capacity and/or powers to consent to the applicable TCUSR;
- That they accept them without reserve.

The Signatory's acceptance is indicated by clicking the checkbox before proceeding to the Document's Signature.

ARTICLE 4 – SIGNATURE-SERVICE DESCRIPTION

The Electronic-Signature Service allows the Signatory to make use of an Electronic-Signature creation solution and allows the Client to collect said signature.

4.1. Signatory's Access to the Service

The Signatory may benefit from the Service offered as long as they have:
- Suitable computer equipment to access the Service;
- A valid and personal email address (for which they control access);
- A means of personal authentication accepted by Universign (e.g., personally attributed cell-phone number).

Level-2 and 3 Electronic Signatures require the issuance of a Certificate for which the Holder is the Signatory.

4.2. Creation of a User Account (personal account)

Access to the Service and its use require the creation of a User Account (personal account)

By way of exception, the level-1 Electronic signature does not require the creation of a User Account for the Signatory.

4.3. Signature-journey description

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

Step 1: Provision of the Document

The Client, via their Workspace, makes available the Document to be signed and, if applicable, attaches a Document to read, for the Signatory.

Step 2: Invitation to sign

The Signatory is invited to sign the Document via the Service If necessary, an address containing a hyperlink facilitating access to the Service is delivered to the Signatory.

Step 3: Acceptance of the TCUSR

The Signatory must read and accept these TCUSR in order to access the Document to be signed, therefore acknowledging their validity and enforceability.

The Signatory's acceptance is indicated when they check the acceptance checkbox provided for this purpose.

Acceptance of the TCUSR is mandatory in order to use the Signature Service.

Step 4: Access to the Document

The Signatory is then directed to an interface displaying the Document to be signed. They are invited to read the Document in its entirety.

Step 5: Signature – Authentication

If they wish to sign, the Signatory clicks on the "sign" button to activate the Signature. To ensure the reliability of the

Signature, the Signatory receives a confidential code delivered to the telephone number they have declared to Universign, to the Client, or which they have completed themselves on the interface before proceeding to the Signature of a Document.

Upon receipt of the authentication code, the Signatory authenticates themselves by entering this code in order to create the Electronic Signature of the Document.

The Signatory is informed and recognizes that the conditions for the collection of their Electronic Signature are suitable and sufficient to produce legal effects and that the Electronic Signature may be validly used against them by a Client or any other third party with an interest in doing so.

4.4. Limitations of use

The Signatory undertakes to carry out the steps making up the Electronic Signature themselves and in accordance with the TCUSR. The delegation of these operations, the delegation of signature, and signature per procurationem are prohibited.

4.5. Signature-Levels description

4.5.1. Level-1 Electronic Signature

For the implementation of the level-1 Signature, 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.

4.5.2. Level-2 Electronic Signature

As part of the implementation of the level-2 Electronic Signature, the Signatory must create a User Account (personal account).

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 the Client), as applicable.

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.

4.5.3. Level-3 Electronic Signature

As part of the implementation of the level-3 Electronic Signature, the Signatory must create a User Account (personal account).

Universign or a Delegated Registration Operator verifies the Signatory's identity in person and by means of an identity document.

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

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.

ARTICLE 5– STORAGE OF SIGNED DOCUMENTS

In certain situations, following Signature operations, Universign may offer to store Documents signed via the Service in such a way as to preserve their integrity.

Storage allows the Client to consult signed Documents online, and ensures their Conservation, return, and/or destruction.

In order to activate the Storage Service, the Signatory must first have created a User Account (personal account).

ARTICLE 6 – SIGNATORIES' OBLIGATIONS

The Signatory undertakes to:

- Provide Universign with exact information for the use of the Service, in particular its identification and authentication data (full name, email address, telephone number, etc.);
- Provide a non-falsified identity document
- Ensure the confidentiality of the confidential code(s) delivered thereto.

ARTICLE 7 – PRE-SIGNATURE REVIEW SERVICE

The pre-Signature Review Service allows a Reviewer to review a Document within the functional journey, before it is presented to a Signatory for signature.

7.1. Review-journey description

The review process is based on the following steps:

Step 1: Provision of the Document to be reviewed

The Client, via their Workspace, makes available the Document to be reviewed and, if applicable, attaches a Document to read, for the Reviewer.

Step 2: Invitation

The Reviewer is invited to review the Document via the Service If necessary, an address containing a hyperlink facilitating access to the Service is delivered to the Reviewer.

Step 3: Acceptance of the TCUSR

The Reviewer must read and accept these TCUSR in order to access the Document to be signed, therefore acknowledging their validity and enforceability.

The Reviewer's acceptance is indicated when they check the acceptance checkbox provided for this purpose.

Acceptance of the TCUSR is mandatory in order to use the Review Service.

Step 4: Access to the Document

The Reviewer is then directed to an interface displaying the Document to be reviewed. They are invited to read the Document in its entirety.

Step 5: Review

If the Reviewer wishes to approve, the Reviewer clicks the "approve" button to activate their approval.

Once approved, the Document is presented to the Signatory for signature, whose details will have been provided by the Client at the time of the review/Signature-journey's creation.

7.2. Applicability to the Reviewer of all other TCUSR clauses applicable to a Signatory

All TCUSR articles not specific to the Signature Service also remain applicable to the review Service.

Article 8– EVIDENCE FILES

Universign will provide Signatories 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 the Signatory upon simple request addressed to Universign Support.

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.

Evidence files also include data extracted from events which contribute to establishing proof of a Reviewer's review operations.

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

ARTICLE 9 – LIABILITY

Universign's intervention is limited to a technical service, providing Signatories with software and technical tools allowing them to benefit from the Service.

Universign undertakes to provide all reasonable care in the performance of the Services, in accordance with best practices, but may only be held to an obligation of means with regard to the Signatory.

Universign's liability may not be sought in case of use of the Service which does not comply with the TCUSR and, more generally, with the policies applicable to the Services.

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.

Any damage to third parties is deemed indirect damage

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 sum of 150 euros for Signatories.

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

ARTICLE 10– SECURITY

Universign undertakes to implement technical, legal, and organizational measures to secure the Service.

As part of their access to the Service, the Signatory is expressly reminded that the internet is not a secure network. Under these conditions, the Signatory is responsible for taking all appropriate measures to protect their own data and/or software from, for example, any alteration and contamination by viruses circulating on the internet and from third-party intrusion into their 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.

ARTICLE 11 – 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 Clients and exceptions related to applicable legal and regulatory provisions.

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

ARTICLE 12– POLICIES AND STANDARDS

As part of the issuance of Certificates prior to high-level Signatures, 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	ETSI EN 319-411-2	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.

ARTICLE 13 – PERSONAL DATA

As part of the Signature Services it provides hereunder, Universign collects and processes Signatory personal data as data controller.

13.1. Personal-Data collection

The legal grounds for Personal-Data Processing carried out as part of the Electronic Signature are:

-the performance of the Contract with a Client with regard to the receipt of Personal Data
-the Signatory's consent to the Processing of their Personal Data which is mandatory in order to use the Electronic-Signature Service The absence of consent will therefore result in Universign's inability to finalize a Signature operation.

Purposes	Data storage periods before deletion
Allowing the Signatory to sign a Document	60 days as of the creation of the Signature Collection by the Client
To store evidence of electronic transactions for the purposes of supervisory-authority audits or to produce in case of dispute	15 to 99 years according to applicable contractual conditions with the Client
To provide technical support and allow the proper functioning of the service and its security in case of request to Universign Support	5 years after the end of the Contract with the Client
To improve our Services and adapt their features and develop new ones	12 months after the end of the Client's relationship with Universign
Allowing Universign to comply with its legal obligations, resolve any disputes and have its contracts respected	Duration defined in the policies applicable to its Services

For increased-level Electronic-Signature Services requiring the prior creation of a Signatory Certificate, a User Account (Personal Account) must be created and the PDPP must be accepted.

The Signatory Personal Data used as part of Signature Services is collected:

•directly from a Signatory after they have consented to the Processing of their Personal Data and/or,
•by the Client who requests that a Signatory sign one or several Documents via the Platform,

13.2. Categories of Personal Data processed

The categories of Signatory Personal Data collected from the latter or transmitted by a Client according to the use of the Service and processed by Universign include:

•identification and contact details (full name, email address, telephone number);
•information sent by the Signatory or the Client, as applicable, to Universign Support;
•information concerning the computer and connection environment, i.e., the IP address, technical IDs, error reports and execution data;
•usage data, such as the data on which the Signatory has clicked, including the date and time of the page's consultation;
•service log-in details (username and password);
•the Signatory's ID with the Client (client number for example).

13.3. Purposes of Personal-Data Processing.

As part of the Electronic-Signature Services, Signatory Personal Data is used to:

•allow a Signatory to sign a Document
•store evidence of electronic transactions for the purposes of supervisory-authority audits or to produce in case of dispute
•provide technical support and allow the proper functioning of the Service and its security in case of request to Universign Support
•improve our Services and adapt their features and develop new ones
•allow Universign to comply with its legal obligations, resolve any disputes and have its contracts respected

13.4. Personal-Data retention periods

All Personal-Data collected is retained for a limit duration according to the processing purpose and the retention period provided for by the laws applicable to our services.

Upon the expiry of the indicated periods, the data will be archived for a duration not exceeding those prescribed by regulations applicable to archiving, if necessary

13.4. Personal-Data recipients and transfers

Outside of the cases provided for by these TCUSR, Signatory Personal Data will never be sold, shared, or communicated to third parties by Universign.
When a Signatory access the Signature Service via a subscription administered by a Client, the Personal Data and certain usage data collected by the Service may be accessible and shared with the Client's administrator in order to analyze use, manage the service's subscription, or provide technical assistance.

Signatories' Personal Data may be communicated to sister companies or subsidiaries, as well as to service providers acting upon Universign's instructions for the sole purpose of carrying out the processing for which it was initially collected. In this context, these service providers are Data Processors within the meaning of applicable regulations, and they act upon the instructions and on behalf of Universign. They are not permitted to sell or disclose said data to other third parties.

To ensure the provision of the Signature Service around the world, particularly with regard to the delivery of SMSs containing confidential codes allowing an Electronic-Signature service Signatory to be identified, Personal Data may be transferred to subcontracted service providers outside of the European Union.

In this case, Universign signs the standard contractual clauses approved by the European Commission with said subcontractor service providers and implements all relevant measures to guarantee adequate protection for the transfer of Personal Data.

As part of audits or other pre-litigation or litigation proceedings, certain Signatory Personal Data may also be shared with other Service users (Client, Partner) to confirm or demonstrate the validity of the Electronic Signatures that a Signatory was able to make through the Universign Service. In this context, only the Personal Data that may be used to prove the validity of the Signature operation will be transmitted.
Furthermore, if a Signature accesses the Universign Services via a third-party application, their Personal Data may be shared with the publisher of this third-party application so that they latter may provide them with access to the application, under the terms of a license and a confidentiality policy specific to said publisher.
Finally, Signatory Personal Data may be disclosed if Universign is so required by law or by a regulatory provision, or if said disclosure is necessary as part of a judicial or administrative request.

13.5. Security and confidentiality

Universign implements all measures to preserve the quality, confidentiality and integrity of processed Personal Data.
Universign uses technical measures (networks protected by standard devices such as firewalls, network partitioning, adapted physical hosting, etc.) and organizational measures (strict and registered access control, procedures, security policy, etc.) to ensure the security and confidentiality of collected Personal Data.
During the processing of Signatory Personal Data, Universign takes all reasonable measures to protect against any loss, misuse, unauthorized access, disclosure, alternation, or destruction.
Individuals with access to Signatory Personal Data are bound to an obligation of confidentiality, and will be exposed to disciplinary measures, and/or engage their liability if they do not respect these obligations.

13.6. Data-protection officer

Universign has named a Data-Protection Officer charged with supervising the protection of personal data and respect for legal and regulatory requirements in this regard.

For any further information or complaint regarding the application hereof or Processing regarding Signatory Personal Data, the latter may be contacted at the address: privacy@universign.com.

In case of any unresolved difficulty regarding the use of its Personal Data the Signatory may also call upon the French Data-Protection Authority (CNIL).

13.7. Right of access, correction, deletion and objection

Whenever Personal Data is processed by Universign, the latter takes all reasonable measures to ensure the accuracy and relevance of Personal Data with regard to the purposes for which it is collected, and guarantees that a Signatory may exercise their rights over said data.
A Signatory has a right of access to their Personal Data, the right to correct it if it is incorrect and, as applicable and according to the limitations provided for by the regulations, to objection and deletion of certain Personal Data, to limit its use or to request its portability with a view to its transmission to a third party.
For any question regarding the application of these rights, the Signatory may contact the Data-Protection Officer at the address:

Universign - Data-Protection Officer
7 Rue du Faubourg Poissonnière 75009 Paris.

The signed request must be delivered by mail with acknowledgement of receipt and include a copy of the Signatory's identity document. This method allows Universign to ensure that the Signatory is the originator of the request.

ARTICLE 14 – 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 TCUSR 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.

Access to contractual documents: The Signatory is informed that only the TCUSR and the other contractual documents described in the article "Contractual documents" are applicable within the context of the Services' performance.

It should be noted that all TCUSR 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 TCUSR 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.

Notification: Any Signatory 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 Universign Support.

ARTICLE 15 – APPLICABLE LAW AND JURISDICTION

These TCUSR, as well as the relationship between the Signatory 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.

Signatories, 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 Signatory 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 TCUSR.