Terms and Conditions (Signatory, Validator)

The purpose of these General Terms and Conditions of Use (hereinafter the "**General Terms and Conditions of Use (Signatory, Validator)**" or "**GTCUS**") is to define the legal conditions applicable to signatories wishing to sign Documents from the Platform made available by Cryptolog International, RCS Paris n° 439 129 164 (hereinafter "**Universign**") via its Customers or Partners.

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.

Certification Authority or CA: designates the authority in charge of creating, issuing, managing and revoking Certificates under the Certification Policy.

Certificate: refers to the electronic file issued by the Certification Authority containing the identification details of its Subscriber and a cryptographic key enabling verification of the Electronic Signature or Electronic Seal for which it is used.

Qualified Certificate: means a Certificate meeting the requirements of Article 28 or 38 of European Regulation n°910/2014 of July 23, 2014.

Electronic Seal or 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).

Collection: refers to the Customer's action of sending one or more Documents to the Universign Platform to be signed by one or more Signatories.

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.

Preservation: refers to the associated Service consisting of the implementation of procedures and technologies enabling the reliability of Electronic Signatures to be extended during the period in which signed Documents are stored by Universign.

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

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

Personal data means any information relating to an identified or identifiable person, directly or indirectly.

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

Workspace: refers to the computer resources allocated to the Customer by Universign and which enable the Customer to invite Signatories to sign a Document.

Delegated Registration Operator or DRO means a natural person who carries out Certificate Holder registration operations on behalf of and on the instructions of Universign, and consequently verifies the identity of the Certificate Holder in his presence (and therefore by carrying out a "face-to-face" operation) and the constitution of 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-sensitive 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.

Personal Data Protection Policy or in presents information relating to 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.

Subscriber means the natural person identified in the Certificate who has under his control the private key corresponding to the cryptographic key shown on the Certificate.

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.

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.

Service(s): refers to Universign's Electronic Signature service made available to the Signatory via a Customer.

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

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 Universign's Storage Service for Signatory's Signed Documents.

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

Processing of Personal Data means any operation or set of operations involving Personal Data, regardless of the process used.

Validator: means a natural person using the Platform to validate a Document before it is put up for signature by a Signatory.

ARTICLE 1 - PURPOSE

These Signatory Terms and Conditions define the conditions applicable to a Signatory using the Electronic Signature Service.

ARTICLE 2 - CONTRACTUAL DOCUMENTS

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

- The Service policies published on the Website ;

- The present CGUSV ;

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 General Terms and Conditions at any time and without prior notice.

The applicable General Terms and Conditions of Use are permanently accessible on the Website, in a format that allows them to be printed and/or downloaded.

ARTICLE 3 - ACCEPTANCE

Prior to any use of the Service, the Signatory acknowledges:

- Have read the applicable CGUSV ;

- Have the legal capacity and/or authority to enter into commitments under the applicable CGUSV;

- Accept without reservation.

The Signatory's acceptance is materialized by clicking on the checkbox before proceeding to Sign a Document.

ARTICLE 4 - DESCRIPTION OF THE SIGNATURE SERVICE

The Electronic Signature Service provides the Signatory with a solution for creating an Electronic Signature and enables the Customer to collect it.

4.1. Signatory's access to the Service

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

- Suitable computer equipment to access the Service;

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

- A means of personal authentication accepted by Universign (e.g. a personally assigned cell phone number).

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

4.2 Creating a User Account (personal account)

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

As an exception, level 1 Electronic Signature does not require the Signatory to create a User Account.

4.3. Signature path description

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

Step 1: Document availability

The Customer, via his Workspace, makes the Document to be signed and, if necessary, adds a Document to be read, available to the Signatory.

Step 2: Invitation to sign

The Signatory is invited to sign the Document via the Service. Where appropriate, an address containing a hyperlink to the Service is sent to the Signatory.

Step 3: Acceptance of the CGUSV

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

The Signatory's acceptance is evidenced by checking the acceptance box provided for this purpose.

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

Step 4: Document access

The Signatory is then directed to an interface displaying the Document to be signed. The Signatory is invited to read the entire Document.

Step 5: Signature - Authentication

If he/she wishes 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 sent

to the telephone number he/she has declared to Universign, to the Customer or which he/she has entered on the interface before signing a Document.

On receipt of the authentication code, the Signatory authenticates himself by entering this code to create the Electronic Signature of the Document.

The Signatory is informed and acknowledges that the conditions under which his Electronic Signature is collected are suitable and sufficient to produce legal effects and that his Electronic Signature may be validly used against him by a Customer or any other third party having an interest in opposing him.

4.4. Limits of use

The Signatory undertakes to carry out the steps constituting the Electronic Signature in accordance with the CGUSV. Delegation of these operations, delegation of signature and signature to order are prohibited.

4.5. Description of Signature Levels

4.5.1. Level 1 electronic signature

As part of the implementation of the Level 1 Signature, 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).

4.5.2. Level 2 electronic signature

To implement Level 2 Electronic Signature, the Signatory must create a User Account (personal account).

The Signatory's identification is checked remotely by means of a 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 the Customer), where applicable.

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.

4.5.3. Level 3 electronic signature

To implement level 3 Electronic Signature, the Signatory must create a User Account (personal account).

Universign or a Delegated Registrar verifies the identity of the Signatory in his presence and with 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 Customer), where applicable.

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

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.

ARTICLE 5 - STORAGE OF SIGNED DOCUMENTS

In certain cases, Universign may offer to store the Documents signed using the Service in such a way as to preserve their integrity.

Storage allows the Customer to consult signed Documents online, to keep them, return them and/or destroy them.

To activate the Storage Service, the Signatory must first create a User Account (personal account).

ARTICLE 6 - OBLIGATIONS OF THE SIGNATORY

The Signatory undertakes to :

- Provide Universign with accurate information for the use of the Service, in particular identification and authentication data (surname, first name, e-mail address, telephone number, etc.);

- Provide unforged identification

- Ensure the confidentiality of the confidential code(s) sent to him/her.

ARTICLE 7 - PRE-SIGNATURE VALIDATION SERVICE

The Pre-Signature Validation Service enables a Validator to validate a Document in the functional path before it is put up for signature by a Signatory.

7.1. Description of the validation process

The validation process is based on the following steps:

Step 1: Provision of the document to be validated

The Customer, via his Workspace, makes the Document to be validated and, if necessary, adds a Document to be read, available to the Validator.

Step 2: Invitation

The Validator is invited to validate the Document via the Service. Where appropriate, an address containing a hyperlink to the Service is sent to the Validator.

Step 3: Acceptance of the CGUSV

The Validator must read and accept these CGUSV in order to access the Document to be signed, thereby acknowledging their validity and enforceability.

The Validator's acceptance is evidenced by checking the acceptance box provided for this purpose.

Acceptance of the CGUSV is mandatory in order to use the Validation Service.

Step 4: Document access

The Validator is then directed to an interface displaying the Document to be validated. The Validator is invited to read the entire Document.

Step 5: Validation

If he wishes to validate, the Validator clicks on the "validate" button to activate the validation.

Once validated, the Document is signed by the Signatory who will have been entered by the Customer when creating the validation/Signature path.

7.2. Application to the Validator of all other clauses of the CGUSV applicable to a Signatory

All articles of the CGUSV that are not specific to the Signature Service also apply to the Validation Service.

ARTICLE 8 - PROOF FILES

Universign will provide Signatories with the data extracted from its event logs used to 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 the Signatory on simple request addressed to Universign Support.

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 proof files will also include data extracted from events used to establish proof of validation operations by a Validator.

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.

ARTICLE 9 - LIABILITY

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

Universign undertakes to take all reasonable care in the performance of the Services in accordance with the best practices of its profession, but shall only be bound by an obligation of best endeavours towards the Signatory.

Universign cannot be held responsible for any use of the Service that does not comply with the CGUSV and, more generally, with the policies applicable to the Services.

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.

Any damage to a third party is considered indirect damage.

In the event of Universign being 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 sum of 150 euros for the Signatories.

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

ARTICLE 10- SAFETY

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

When accessing the Service, the Signatory is expressly reminded that the Internet is not a secure network. Under these conditions, it is the responsibility of the Signatory to take all appropriate measures to protect his or her 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 his or her 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.

ARTICLE 11 - 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 unrelated to the provision of the Service, other than to Customers and other than in accordance with applicable laws and regulations.

This provision does not preclude judicial or administrative communications.

ARTICLE 12 - POLICIES AND STANDARDS

When issuing Certificates prior to a High-Level Signature, 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**	**PC for LCP-level certificates for natural**

1.3.6.1.4.1.15819.5.1.3.1	E T S I E N 3 1 9 - 4 1 1 - 2	PC for certificates of natural persons, leve

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

ARTICLE 13 - PERSONAL DATA

In the context of the Signature Services it provides hereunder, Universign collects and processes Signatories' personal data in its capacity as data controller.

13.1. Collection of Personal Data

The legal bases for the Processing of Personal Data carried out within the framework of the Electronic Signature are :

-the performance of a contract with a customer as regards the receipt of Personal Data

-the Signatory's consent to the Processing of his Personal Data, which is mandatory in order to use the Electronic Signature Service. The absence of consent will make it impossible for Universign to finalize a Signature operation.

For high-level Electronic Signature Services requiring the prior creation of a Certificate, the Signatory must create a User Account (Personal Account) and accept the PPDP.

A Signatory's Personal Data used for Signature Services is collected :

-directly to a Signatory after he has consented to the Processing of his Personal Data and/or,

-by the Customer who asks a Signatory to sign one or more Document(s) via the Platform,

13.2 Categories of Personal Data Processed

The categories of Personal Data of the Signatory that are collected from him, transferred by a Customer depending on the use of the Service and processed by Universign include:

identification and contact data (surname, first name, e-mail address, telephone number);

-information sent by the Signatory or the Customer to Universign Support;

-information about the computer, the connection environment, i.e. IP address, technical identifier(s), error reports and execution data;

-Usage data, such as data on which the Signatory has clicked, including the date and time the page was consulted;

-Service login details (user name and password) ;

-the customer's Signatory ID (e.g. customer number).

13.3 Purpose of Personal Data Processing

As part of the Electronic Signature Services, the Signatory's Personal Data is used for :

-allow a Signatory to sign a Document

-Keep evidence of electronic transactions for auditing purposes by supervisory authorities or for production in the event of litigation

-provide technical support and enable the Service to operate and be secured in the event of a request to Universign Support

-Improve our services, adapt their functionalities and develop new ones.

-Universign can comply with its legal obligations, resolve any disputes and enforce its contracts.

13.4. Retention periods for Personal Data

All Personal Data collected is kept for a limited period of time depending on the purpose of the processing and the retention period stipulated by the legislation applicable to our services.

At the end of the periods indicated, the data will, if necessary, be archived for a period not exceeding the periods prescribed by the applicable archiving regulations.

Goals	Data retention periods before deletion
Allow the Signatory to sign a Document	60 days from the creation of the Signature Collection by the Customer

Keep evidence of electronic transactions for auditing purposes by supervisory authorities or for production in the event of litigation	From 15 to 99 years depending on the contractual terms applicable with the Customer
Provide technical support and ensure the smooth operation of the service and its security in the event of a request to Universign Support.	5 years after the end of the Contract with the Customer
Improve our services, adapt their functionalities and develop new ones.	12 months after the end of the Customer's relationship with Universign
So that Universign can comply with its legal obligations, resolve any disputes and enforce its contracts	Duration defined in the policies applicable to its Services

13.4. Recipients and transfers of Personal Data

Apart from the cases provided for in the present CGUSV, the Personal Data of Signatories will never be sold, shared or communicated to third parties by Universign.

When a Signatory accesses the Signature Service through a subscription administered by a Customer, Personal Data and certain usage data collected by the Service may be accessed and shared with the Customer's administrator for the purposes of analyzing usage, managing the service subscription or providing technical assistance.

The Personal Data of Signatories may be communicated to sister companies or subsidiaries as well as to service providers acting on the instructions of Universign for the sole purpose of carrying out the processing for which they were initially collected. In this context, these service providers are personal data processors within the meaning of the applicable regulations, acting on the instructions and on behalf of Universign. They are not authorized to sell or disclose your personal data to other third parties.

Personal Data may be transferred to subcontractors located outside the European Union in order to ensure the provision of the Signature Service throughout the world, in particular the sending of SMS messages containing confidential codes enabling Signatories of the Electronic Signature service to identify themselves.

In this case, Universign concludes standard contractual clauses approved by the European Commission with these subcontractors and implements all relevant measures to guarantee an adequate protection framework for the transfer of Personal Data.

In the context of audits or pre-litigation or litigation proceedings, certain Personal Data of Signatories may also be shared with other users of the Service (Customer, Partner) to confirm or demonstrate the validity of Electronic Signatures that a Signatory may have carried out using the Universign Service. In this context, only Personal Data useful for proving the validity of the Signature operation will be transmitted.

Furthermore, if a Signatory accesses the Universign Service(s) via a third-party application, their Personal Data may be shared with the publisher of this third-party application so that the latter can provide them with access to the application, under the terms of a license and privacy policy specific to this publisher.

Finally, the Signatory's Personal Data may be disclosed if Universign is required to do so by law or regulation or if such disclosure is necessary in connection with a judicial or administrative request.

13.5. Security and confidentiality

Universign makes every effort to preserve the quality, confidentiality and integrity of the Personal Data processed.

To ensure the security and confidentiality of the Personal Data collected, Universign uses technical means (networks protected by standard devices such as firewalls, network partitioning, adapted physical hosting, etc.) and organizational means (strict and nominative access control, procedures, security policy, etc.).

When processing the Signatory's personal data, Universign takes all reasonable steps to protect it from loss, misuse, unauthorized access, disclosure, alteration or destruction.

Persons with access to Signatories' Personal Data are bound by an obligation of confidentiality, and may be subject to disciplinary action and/or liability if they fail to comply with these obligations.

13.6. Data Protection Officer

Universign has appointed a Data Protection Officer to ensure the protection of personal data and compliance with legal and regulatory requirements.

For any further information or complaint concerning the application of the present Terms and Conditions or the Processing of the Signatory's Personal Data, the latter may contact him at the following address: **privacy@universign.com** .

In the event of unresolved difficulties relating to the use of Personal Data, the Signatory may also refer the matter to the CNIL.

13.7. Right of access, rectification, deletion and objection

Whenever Personal Data is processed by Universign, Universign takes all reasonable steps to ensure the accuracy and relevance of the Personal Data with respect to the purposes for which it is collected and to ensure that a Signatory can exercise its rights with respect to such data.

A Signatory has the right to access his or her Personal Data, the right to rectify it if it is inaccurate and, in the cases and within the limits provided for by the regulations, the right to object, to delete some of this Personal Data, to limit its use or to request its portability with a view to its transmission to a third party.

For any questions relating to the application of any of these rights, the Signatory may contact the Data Protection Officer at the following address:

Universign - Data Protection Officer

7 rue du Faubourg Poissonnière 75009 Paris.

The signed request must be sent by post with acknowledgement of receipt and include a copy of the Signatory's identity document. This procedure enables Universign to ensure that the Signatory is the originator of the request.

ARTICLE 14 - 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.

If any clause of these GCUSV is held to be invalid or unenforceable by law, regulation or court decision, it shall be deemed to be unwritten and the remaining clauses shall remain in full force and effect.

Access to contractual documents : The Signatory is informed that only the CGUSV 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 CGUSV 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 CGUSV 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.

Notification: Any complaint or notification from a Signatory must be sent to Universign by post to its registered office at 7 rue du Faubourg Poissonnière 75009 Paris or via Universign Support.

ARTICLE 15 - APPLICABLE LAW AND JURISDICTION

These GCUSV and the relationship between the Signatory 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 accessory 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.

Signatories 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 Signatory and Universign agree to submit to the exclusive jurisdiction of the competent courts of Paris in order to resolve any dispute relating to the validity, performance or interpretation of the GCUSV