TERMS AND CONDITIONS FOR THE ADVANCED ELECTRONIC SIGNATURE SERVICE

1. PREAMBLE

The purpose of these Terms and Conditions is to define the legal terms applicable to the service allowing the collection and recording of the Signatory's consent to an Electronic Document issued by the financial institution using an Advanced Electronic Signature based on an electronic Certificate (hereinafter referred to as the "Service").

As part of the Service:

DocuSign France is the Certification Authority (CA) responsible for:

- Issuing the Signatory's Certificate,
- Electronically sealing the Electronic Document presented to the Signatory using the private key associated with the Signatory's Certificate in a secure signature creation device.

The financial institution is the Registration Authority (RA) responsible for:

- Authenticating Signatories,
- Presenting the Electronic Document,
- Collecting the Signatory's consent for the issuance of the Certificate and the electronic signature of the Electronic Document.

Quicksign is the Technical Service Provider of the Registration Authority (TPRA) responsible for:

- Coordinating with the CA the lifecycle of Certificates and technical connections,
- Performing some identity verifications outsourced by the RA,
- Generating a Proof File associated with the signature of the Electronic Document,
- Transmitting the Proof File to the archiving third party, if applicable.

2. DEFINITIONS

Certification Authority (CA): Refers to DocuSign France, the entity that issues the Certificates, manages their lifecycle at the request of the Registration Authority in accordance with the rules and practices defined in the Certification Policy, and signs the hash of the Electronic Document to be signed with the private key associated with the issued Certificate. The applicable Certification Policy can be viewed on the CA's website: https://www.docusign.fr/societe/politiques-de-certifications ("PROTECT & SIGN" Certification Policy).

Registration Authority (RA): Refers to the entity responsible for verifying and authenticating the Signatory's identity, collecting the information used within the Consent Protocol to ensure that the consent is under the exclusive control of the Signatory (such as the Signatory's mobile phone number to send the OTP Code), and submitting the Certificate request to allow the Signatory to sign the Electronic Document. The RA is responsible for defining the rules for verifying and authenticating the Signatories' identities. The RA may delegate all or part of the technical implementation of its identity verification rules to one or more TPRAs. In this context, the RA is the financial institution.

Certificate: Refers to an electronic file that links the electronic signature validation data to the identity of a given Signatory.

Private key: Refers to a unique and secret mathematical key, contained in a signature creation device, hosted and managed by the CA and activated remotely by the Signatory to sign the Electronic Document.

Electronic Document: Refers to the document(s) created by the RA to be signed by the Signatory.

Proof File: Refers to a file generated, signed, and timestamped by the TPRA containing information related to the Signatory's authentication transmitted by the RA and the transcription of the Signatory's consent to sign the Electronic Document (including technical event logs related to consent). A dedicated Proof File is associated with each signed Electronic Document to prove the validity of the electronic signature in case of legal proceedings.

Consent Protocol: Refers to the procedure whereby the RA collects the Signatory's consent for:

- The issuance of a Certificate in their name,
- The acceptance to sign the Electronic Documents.

OTP Code: Refers to a one-time password sent to the Signatory on their mobile phone, enabling the electronic signature process to begin.

Registration Policy: Refers to the set of rules defined by the RA to verify and authenticate the Signatory's identity and collect registration information used to issue the Certificate.

Technical Service Provider of the Registration Authority (TPRA): Refers to the service provider responsible for collecting the Signatory's contact and identity information, carrying out part of the technical identity verification measures outsourced by the RA, sending the Certificate issuance request and the documents to be signed to the CA, creating the Proof File, sealing it, timestamping it, and making it available to the RA. In this context, the TPRA is QuickSign.

Signatory: Refers to any individual signing an Electronic Document using the Service.

Advanced Electronic Signature: Refers to an advanced electronic signature as defined in Article 3-11 of the European regulation 910/2014 ("eIDAS").

3. PURPOSE OF THE SERVICE

The Service allows:

- The collection and recording of the Signatory's consent to an Electronic Document using an Advanced Electronic Signature associated with a Certificate.

- The creation of a Proof File to log events related to the Advanced Electronic Signature act.

The Electronic Document signed with an Advanced Electronic Signature through the Consent Protocol is legally binding. Indeed, eIDAS states that an Advanced Electronic Signature carried out via the Service cannot be denied solely because it is in electronic form.

4. DESCRIPTION OF THE SERVICE

The Signatory is informed and expressly agrees that:

- The RA identifies the Signatory in compliance with the rules it has defined or to which it is subject under regulatory constraints related to anti-money laundering and counter-terrorism (AML).

- The RA collects the Signatory's identity information and contact details (first name, last name, mobile phone number, email address, date of birth, and any proof of identity).

- The RA creates an Electronic Document to be signed by the Signatory.

- The TPRA transmits the identity information and the Electronic Document to the CA to carry out the Advanced Electronic Signature operations.

- The CA issues the Certificate and proceeds to sign the Electronic Document using the private key associated with the Certificate.

Thus, the Signatory is informed and expressly agrees that:

- A Certificate and a private key will be assigned to them by the CA in accordance with its applicable Certification Policy.

- The Signatory must express their consent through checkboxes and by entering the OTP code in accordance with the Consent Protocol.

- The TPRA generates a Proof File containing a log of events associated with the signature of the Electronic Document. The RA is responsible for storing the Proof File.

5. SIGNATORY OBLIGATIONS

By agreeing to use the Service, the Signatory agrees to comply with the Terms and Conditions and to:

- Provide accurate and authentic identity information,

- Protect the security and confidentiality of the information used to activate the Consent Protocol (such as the OTP Code) and, if the code is temporary (such as an OTP Code), destroy it after the signing process,

- Verify the identity information contained in the Certificate and alert the RA if the Certificate has been incorrectly completed,

- Promptly inform the RA of any changes in identity information to be included in the Certificate or in the Electronic Document,

- Use the Service only to sign Electronic Documents created by the RA.

The RA, TPRA, and CA are not responsible for any harmful consequences resulting from the Signatory's failure to provide accurate and truthful information.

6. CERTIFICATE PUBLICATION

The Certificate is not published by the CA or RA. The Certificate is contained in the signed Electronic Document and in the Proof File associated with the Electronic Document.

7. EVIDENCE MANAGEMENT

The Signatory agrees that the elements used for the purposes of the Service, particularly the information used during the execution of the Consent Protocol, the Certificate, and supporting documents (e.g., a copy of the identity document used to identify the Signatory), may be used as evidence in legal proceedings.

8. EFFECTIVE DATE AND DURATION

These Terms and Conditions shall take effect on the date they are presented to the Signatory, which coincides with the date of the Certificate issuance request.

9. APPLICABLE LEGAL SYSTEM, PROCEDURES, CLAIMS, AND DISPUTE RESOLUTION

The Terms and Conditions, their validity, interpretation, and execution are governed by French law. Any dispute relating to the validity, interpretation, and execution of all or part of these Terms and Conditions shall be subject to the jurisdiction of the courts of Paris.