docusign™

TERMS OF USE – DOCUSIGN EU QUALIFIED SIGNATURE SIGNER CERTIFICATE

These Terms of Use were last updated on **October 30, 2023**.

If an agreement exists between You and DocuSign for EU Qualified Signature (“**Agreement”**), then, in the event of any inconsistency or conflict between these Terms of Use and the Agreement, the Agreement shall control with respect to DocuSign EU Qualified Signature.
These Terms of Use (“**Terms**”) apply to a signer’s (“**Signer**,” “**You**,” or “**You**r”) use of the Service and the Certificate delivered by DocuSign France SAS, Central Park - 9-15 rue Maurice Mallet - 92130 Issy-les-Moulineaux, France (“**DocuSign**”). By clicking that you accept these terms in the DocuSign Signature Application product workflow (“**DocuSign Signature Application**”), You indicate Your acceptance of these Terms and You agree to be bound by the Terms as of the date of Your acceptance (“**Effective Date**”).

Certificates are generated and managed in the context of the online qualified electronic signature service provided by DocuSign to the Customer.

DocuSign France Customer Service is available from Monday to Friday, from 9am to 6pm, working days in France, except on legal holidays. It can be reached using https://support.docusign.com/s/contactSupport?language=en_US&langSet=1.

1. DEFINITIONS

“Certificate(s)” means a qualified certificate for electronic signature as defined in Article 3-15 eIDAS and as generated by DocuSign to confirm the connection between Your identity and Electronic Signature Creation Data. The Certificate is used for Your electronic signature (via the Service and under these Tems) of an eDocument addressed thereto.

“Certification Authority (or CA)” means the authority that generates and manages Certificates in accordance with the rules and practices defined in the Certificate Policy(ies). For the purpose of these Services, the CA is DocuSign France SAS, listed as “DocuSign Premium Cloud Signing CA - SI1” with The National Cybersecurity Agency of France **(“ANSSI”).**

“Certificate Policy(cies) (or CP)” means the set of security rules for the TSP stipulated by an OID and published by the CA. DocuSign’s Certificate Policy and any successive updates are designated as 1.3.6.1.4.1.22234.2.14.3.45 and available at: https://www.docusign.fr/societe/certification-policies.

“Consent Protocol” means the procedure via the DocuSign Signature Application and/or Service which You consent to receive a Certificate with the Signer Identity, to accept signing the eDocument via the Service, and to accept consenting to these Terms.

“Customer(s)” means any legal entity or person authorized as a DocuSign customer to use the Service that delivers eDocuments to a Signer. The Customer, as described herein, is distinguishable from You as the Signer.

“Service” means the DocuSign on-demand electronic signature service, which provides online display, certified delivery, acknowledgement, qualified electronic signature, and storage services for eDocuments.

“eDocument(s)” refers to a contract, notice, disclosure, or other record or document generated using or deposited into the DocuSign Service for processing.

“Electronic Signature Creation Data” means secret data that is uniquely contained within a certified remote qualified signature creation device, as defined in Article 3(-23) eIDAS, and remotely activated and used by the signatory to create an electronic signature.

“**ID Document (ID)**” for purposes of the Service means a passport, a national identity card, a residence permit. The ID shall meet the security requirements defined by The National Cybersecurity Agency of France (ANSSI) to qualify for the Service.

“Proof File(s)” means a file generated, signed, and time-stamped by DocuSign that contains information related to the Signer identification and the signature generated by the Service. A dedicated Proof File is associated with each signed eDocument and Terms for proving the validity of the electronic signature. The Proof file is only available to the RA by request in instances of a legal claim or contest of the signature operation.

“Certificate of Completion (or “COC”) means a file generated by the DocuSign Signature Application associated with each eDocument that contains all the information related to the Signer and the sender of the eDocument, including a unique identifier of the Transaction. A dedicated COC is generated to prove the validity of a Transaction.

“**Qualified Signature” (or “QES”)** means qualified electronic signature as defined in Article 3(12) eIDAS.

“Remote Identity Verification Service Provider” (or “RIVSP”) means the third party service provider responsible for capturing a video of Signer’s facial image and ID in order to verify Signer Identity, and for producing the evidence file and sending the Remote Identity Verification Result to the CA. All RVISPs are certified by The National Cybersecurity Agency of France (ANSSI).

“Remote Identity Verification Result” (“RIVR”) means the signed information collected and sent by the RIVSP to the CA, including the verdict (successful or unsuccessful) of the remote identity verification of Signer, the reason for the failure if any, the information required by the CA (Signer Identity, email and mobile phone number of Signer) and extracted information from the Signer’s ID document verified by the RIVSP (Your date of birth, IDs serial number, IDs expiration date, IDs issuing country, and IDs type).

“Service” means IDV Premier for QES within the DocuSign Signature Application.

“Signer(s)” mean(s) any individual who uses the Service to sign eDocument(s) resulting in the delivery of a unique Certificate.

“Signer Identity” is the name officially registered on the Signer’s ID. Signer’s Identity cannot be an alias or a pseudonym. It shall be composed of at least one first name and one last name as stated on the Signer’s ID.

“Transaction(s)” means the performance of a signature process, defined by a set of eDocuments submitted for electronic Signature by one or more Signer(s) within the DocuSign Signature Application.

“Trust Service Provider” (or “TSP”) means an entity certified by an external accredited auditor to offer Certificates for QES and Time Stamps. DocuSign is a TSP certified by the National Cybersecurity Agency of France (ANSSI).

"Identity Wallet" or "ID Wallet" means an optional service offered by DocuSign and DocuSign Inc., to the Signer to securely store Signer Identity, RIVR, and Signer information (email and mobile phone number) for use of Signer Identity in current or future Transactions and signatures of eDocuments without performing multiple PVID identification processes.

2. PROCEDURE FOR REQUESTING CERTIFICATES VIA THE SERVICE

2.1 You acknowledge that DocuSign, following the execution of the Consent Protocol, generates a QES necessary to establish a signed and time-stamped eDocument and a signed and time-stamped version of the Terms. In Order to generate a QES, you acknowledge that the following are necessary:

(a) Your Signer Identity is verified by the RIVSP or by Your utilization of the DocuSign Identity Wallet.

(b) The RIVSP will record limited personal information about You (email, telephone number, or other authentication method that may be allowed) in order to verify Your identity and register such information in the Consent Protocol as required by law.

(c) After verification of the Signer's information, DocuSign will send You an email to invite You to sign the eDocument and the Terms. You may also be asked if you want to create an Identity Wallet. The generated email contains a unique internet address to allow Your access to the eDocument and to execute the Consent Protocol in order to collect Your acceptance or refusal to sign the eDocument and the Terms.

(d) DocuSign generates an Electronic Signature Creation Data to facilitate a QES. This Electronic Signature Creation Data can be assigned to You only for the duration of transaction related to an individual eDocument. The activation of the Private Key to sign the eDocument is kept under Your sole control by verification in the Consent Protocol of a unique temporary code, generated and sent by SMS on Your mobile phone by DocuSign.

(e) DocuSign, acting as the CA, generates a Proof File associated with each signature of an eDocument. DocuSign will provide You, the COC, and the signed eDocuments per automated email upon conclusion of the signing process. The Proof File contains:

- A reference to the eDocument presented to the Signer before signature;
- The signature of the eDocument;
- The RIVR from the RIVSP;
- The date and time of the signature generated by the Service;
- The consent protocol as executed between the Signer and the CA; and
- The Signer's information used to perform the consent protocol and to populate the Certificate.

(f) Once signed by You, the Terms is sent by email indicated in the Consent Protocol to You immediately after the signature process.

3. CERTIFICATE ACCEPTANCE

You must verify the content of the information that is presented to You through the Consent Protocol is correct and accurate. In the event there is incorrect information presented during the verification of information in the Consent Protocol, You shall cancel the signature operation and inform the RA. If You notice a problem in the Certificate content after issuance, You shall immediately report the problem to DocuSign by revoking the Certificate as described in ***Section 6*** below.

4. IDENTITY WALLET

If You have selected the option to create an Identity Wallet, then You will must first create or log into your DocuSign Services Account with Your email and password. DocuSign will securely store Your Signer's Identity, the RIVR and some Signer's Information (email and mobile phone number) for future use associated with Signer's Identity. In addition to Your DocuSign Services

Account, you consent to Docusign requesting the device used by the Signer during the Transaction to securely create and store a secret authentication key that is assigned to You.
When You have been issued an Identity Wallet, You will be able to proceed with additional Transactions requiring QES without doing an identification process with the RIVSP. Each Transaction will require You to use Your device and secret cryptographic authentication key.
Your Signer's Identity Wallet will be active for a maximum of three years, depending on the validity period of the cryptographic authentication key or duration of your identification method being valid. After expiration, You will be required to start the process of creating an Identity Wallet again.
At any time, You may access Your DocuSign account in order to delete the Identity Wallet. Upon deletion, DocuSign will securely destroy Your personal information. As a certified Trust Services Provider, DocuSign is obligated to retain an audit log of all QES activities for up to seven years.

5. CERTIFICATE PERIOD OF VALIDITY

Certificates are valid for ten (10) days, from the date the Certificate is created by the CA. Upon expiration of this validity period, signatures may be verified with the verification software indicated by DocuSign, in order to verify that on the eDocument and Terms date of signature, the Certificate was valid.

6. CERTIFICATE TERMS OF REVOCATION

The Customer and You may request a revocation of the Certificate. Your revocation is subject to the following processes outlined below:

6.1 Revocation At The Initiative Of The Signer

You may revoke the Certificate only during the validity period of the Certificate (10 days) by using the online revocation service provided by DocuSign (located at https://docusign.fr/revocation). You may request a revocation due to the following:

- Your Signer Identity information was incorrect;
- The RIVSP failed to comply with its obligations and with the security rules described in their Terms.
- You suspect fraud, mishandling, or creation of Signature on Your behalf without Your consent.

The Certificate shall be revoked within twenty-four (24) hours after the request verification date and will be contained in the CRL published by CA. The Signer is informed of the Certificate revocation by the CA by email.

6.2 Revocation At The Initiative Of The CA

The Certificate shall be revoked immediately by the CA in the event of one of the following circumstances:

- The CA is revoked;
- Signer or RIVSP failed to comply with the necessary obligations and security rules defined in the CP and RIVSP's policy and in the present Terms;
- The Electronic Signature Creation Data has been or is suspected to be lost or compromised;
- Any other reasons legitimately indicated by the CA.

The affected Signer shall be informed of the Certificate revocation by ANSSI.

7. EFFECTIVE DATE AND DURATION

These Terms are effective from the Effective Date until the expiration of the validity of the Certificate for the applicable Transaction.

8. OBLIGATIONS OF SIGNER

By accepting these Terms, You acknowledge and agree to:

(a) Ensure the security and confidentiality of the temporary code received by SMS to sign the eDocument.

(b) Verify the content of the Certificate and alert DocuSign in case of incorrect information reflected on the Certificate.

(c) Verify the authenticity and accuracy of the information in the Consent protocol.

(d) Promptly request the revocation of a Certificate to the CA as described above, and if You suspect theft, unauthorized disclosure, or other fraudulent activity.

(g) Promptly inform the Transaction owner of any change to the authentication means used by the Signer to receive the temporary code (e.g., Signer's mobile number) and identity and supporting documents used by the RIVSP in order to verify and register the Signer Identity.

(h) Stay informed, via the DocuSign websites, of any changes to Certificate Authority and CRL status.

(i) You shall protect your DocuSign account and are its sole user.

(j) If you elect to create an Identity Wallet that You agree to protect the cryptographic key so that it is only used by You, in Your sole discretion, and in the context of a Transaction authorized by You.

9. LIMITATIONS OF LIABILITY

9.1. NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THESE TERMS, DOCUSIGN WILL NOT, UNDER ANY CIRCUMSTANCES, BE LIABLE TO YOU FOR ANY DIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL, COVER, PUNITIVE, OR EXEMPLARY DAMAGES ARISING OUT OF OR RELATED TO THE USE OF SERVICE OR ID WALLET, INCLUDING, BUT NOT LIMITED TO, GOODWILL, WORK STOPPAGE, LOST PROFITS, OR LOSS OF BUSINESS, EVEN IF APPRISED OF THE LIKELIHOOD OF SUCH LOSSES, AND WHETHER SUCH CLAIMS ARE MADE BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE), OR ANY OTHER LEGAL THEORY.

9.2. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL DOCUSIGN BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES WHATSOEVER RESULTING FROM ANY: (A) PERSONAL INJURY OR PROPERTY DAMAGE OF ANY NATURE WHATSOEVER RESULTING FROM YOUR ACCESS TO AND USE OF THE SERVICE OR ID WALLET; (B) ANY UNAUTHORIZED ACCESS TO OR USE OF THE SERVICE OR ID WALLET, AND/OR ANY AND ALL PERSONAL INFORMATION AND/OR FINANCIAL INFORMATION STORED WITH DOCUSIGN; (C) ANY INTERRUPTION OR CESSATION OF TRANSMISSION TO OR FROM OUR SERVERS; (D) ANY BUGS, VIRUSES, TROJAN HORSES, OR THE LIKE THAT MAY BE TRANSMITTED TO OR THROUGH THE SERVICE OR ID WALLET BY ANY THIRD PARTY; (E) ANY LOSS OF YOUR DATA OR USER CONTENT FROM THE SERVICE OR ID WALLET; (F) ANY ERRORS OR OMISSIONS IN ANY OF YOUR DATA OR USER CONTENT, OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF YOUR USE OF SERVICE OR ID WALLET, TRANSMITTED, OR OTHERWISE MADE AVAILABLE VIA THE SERVICE OR ID WALLET, WHETHER BASED ON WARRANTY, CONTRACT, TORT (INCLUDING NEGLIGENCE), OR ANY OTHER LEGAL THEORY, AND WHETHER OR NOT DOCUSIGN IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES; AND/OR (G) THE DISCLOSURE OF INFORMATION PURSUANT TO THESE TERMS, OUR PRIVACY NOTICE, OR ANY OTHER COMMUNICATION WE MAKE OR NOTICE WE PROVIDE.

10. FORCE MAJEURE

Neither You nor DocuSign will be liable for failure to perform any obligation under these Terms to the extent such failure is caused by a force majeure event (including acts of God, natural disasters, war, civil disturbance, action by governmental entity, strike, and other causes beyond the party's reasonable control). The party affected by the force majeure event will provide notice to the other party within a commercially reasonable time and will use commercially reasonable efforts to resume performance as soon as practicable. Obligations not performed due to a force majeure event will be performed as soon as reasonably possible when the force majeure event concludes.

11. PROTECTION OF PERSONAL DATA

11.1 Any personal information that You provide to DocuSign will be processed in line with DocuSign's Privacy Notice, unless otherwise specified in these Terms. As part of this Service or ID Wallet, personal information is collected for the following purposes: Your authentication and identification as the Signer for the Transaction, the creation and use of an Identity Wallet, and the creation of the Certificate and the Consent Protocol. If You do not consent to DocuSign's collection and/or processing and/or storing, you should not proceed with the use of the Service or ID Wallet.

11.2 DocuSign receives some personal information from the RIVSP and will store it as part of the Certificate. This information cannot be modified as it is identification proof and uniquely tied to the Signer. DocuSign and You may not make changes or adjustments to such personal information, including such information stored as part of Your Identity Wallet.

11.3 DocuSign and RIVSP will retain personal information in line with its Privacy Notice for Docusign and RIVSP's policy as published by RIVSP, and as legally obligated as part of the Proof File. By consenting to the Terms, You, as the Signatory, agree that the DocuSign shall retain a proof file containing its personal data for a period of seven (7) years after the Certificate expires based on the applicable legal and regulatory requirements.

12. INTELLECTUAL PROPERTY

DocuSign, its affiliates, or its licensors own all right, title, and interest in and to any and all copyrights, trademark rights, patent rights, database rights, and other intellectual property or other rights in and to the DocuSign Services and related documentation, any improvements, design contributions, or derivative works thereto, and any knowledge or processes related thereto (including any machine learning algorithms output from the DocuSign Services) and/or provided hereunder.

13. GOVERNING LAW

13.1 If You are acting for professional purposes, the following paragraph shall apply to You: These Terms and any disputes or claims arising out of or in connection with it or its subject matter or formation are governed by and construed in accordance with the laws of France. Each party irrevocably agrees that the commercial courts of Paris shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with these Terms or its subject matter or formation. The provisions of the 1980 U.N. Convention on Contracts for the International Sale of Goods are expressly excluded and do not apply to this Agreement. Any legal action arising under this Terms must be initiated within two years after the cause of action arises.

13.2 If You are not acting for professional purposes, this paragraph shall apply to You to the exclusion of the above paragraph: these Terms and any disputes or claims arising out of or in connection with it or its subject matter or formation are governed by and construed in accordance with the laws of France. The French courts as identified by the applicable rules for jurisdiction where a consumer is a party to a dispute shall have exclusive authority to settle any dispute or claim arising out of or in connection with this Terms or its subject matter or formation.

14. WAIVER

The waiver by either party of any breach of any provision of these Terms does not waive any other breach. The failure of any party to insist on strict performance of any covenant or obligation in accordance with these Terms will not be a waiver of such party's right to demand strict compliance in the future, nor will the same be construed as a novation of these Terms.

15. SEVERABILITY

If any part of these Terms is found to be illegal, unenforceable, or invalid, the remaining portions of these Terms will remain in full force and effect, unless such unenforceable or illegal provision was an essential obligation of DocuSign, in which case, these Terms will terminate.

16. MODIFICATION OF TERMS

DocuSign may revise these Terms, including changing, deleting, or supplementing with additional terms and conditions from time to time in its sole discretion, including to reflect changes in applicable law. The changes are deemed accepted by You if You continue using the Service. In the event that You do not agree with any such modification, You shall discontinue Your use of the DocuSign Services or ID Wallet.

17. ENTIRE AGREEMENT

The Terms are the final, complete, and exclusive expression of the agreement between the parties regarding the Service or ID Wallet provided under these Terms. These Terms supersede, and the parties disclaim any reliance on, all previous oral and written communications (including any confidentiality agreements pertaining to EU Qualified Signature under this Terms, representations, proposals, understandings, and negotiations with respect to the matter hereof) and apply to the exclusion of any other terms that You seek to impose or incorporate, or which are implied by trade, custom, practice or course of dealing.

18. LANGUAGES AND TRANSLATIONS

DocuSign may provide translations of these Terms or other terms or policies. Translations are provided for informational purposes and if there is an inconsistency or conflict between a translation and the English version, the English version will control.