DocuSign

TERMS OF USE – ID CHECK FOR AES

Terms of Use version date: January 10, 2020

If an agreement exists between You and DocuSign for ID Check for AES ("**Agreement**"), then, in the event of any inconsistency or conflict between this Terms of Use and the Agreement, the Agreement shall control with respect to ID Check for AES.

This Terms of Use ("**GTU**") defines the legal terms concerning the acquisition and use by you ("**Signer**," "**You**," and "**Your**") of the Service and associated Certificate delivered via the Service from DocuSign France SAS, having its registered offices at Immeuble Central Park, 9-15 rue Maurice Mallet, 92130 Issy-les-Moulineaux, France registered to the registry of companies under the number 812 611 150 (R.C.S. Nanterre) ("**DocuSign**"), and the respective obligations of the Customer and You. By accepting this GTU or by clicking a box indicating your acceptance of this GTU, You agree to be bound by the terms of this GTU as of the date of Your accepting this GTU ("**Effective Date**"). Certificates are generated and managed in the context of the online advanced electronic signature service provided by DocuSign to the Customer.

1. DEFINITIONS

"Advanced Electronic Signature" (or "AES") means advanced electronic signature as defined in Article 3-11 of eIDAS.

"Certificate(s)" means the Certificate generated by the CA via the Service for a Signer, which attests the unique link between the Signer Information and a Public Key. The Public Key is uniquely associated with a Private Key managed by DocuSign. In this case, the term "Certificate" means the certificate for electronic signature, as defined in Article 3-14 of eIDAS, generated by DocuSign to the benefit of a Signer.

"Certification Authority" (or "CA") is DocuSign, the authority that generates Certificates and manages the Certificate lifecycle (issuance, renewal, revocation) on the request of the Registration Authority, in accordance with the rules and practices defined in its Certificate Policy(ies) and the associated Certification Practice Statement.

"Certificate Policy(ies)" (or "CP") means the set of rules published by the CA. A Certificate Policy describes the general characteristics of the Certificates as well as the obligations and responsibilities of the CA, the RA, Signers, Certificate requesters and any other PKI component involved in the management of a Certificate lifecycle. The Certificate Policy(ies) of DocuSign and its (their) successive update(s) can be accessed on DocuSign's website (https://www.docusign.fr/societe/certification-policies), and are an integral part of this GTU. For the purposes of this GTU, the applicable OID is 1.3.6.1.4.1.22234.2.14.3.32.

"**Certificate Revocation List" (or "CRL")** means the list of invalid Certificates that have been revoked before their expiration date. CRLs are issued periodically and are digitally signed by the CA that issued the Certificates in the list. The URL for where to find the CRL is contained in the Certificate.

"Consent Protocol" means the procedure within the Service accessible via DocuSign Signature by which You consent to receive a Certificate with the Signer Information, to accept signing the eDocument via the Service, and to accept this GTU.

"Customer(s)" means any legal entity or person(s) authorized as a DocuSign customer to use the Service that delivers an eDocument(s) to be signed by a Signer via the Service. The Customer, as described herein, is distinguishable from You as the Signer.

"DocuSign Signature" means DocuSign's on-demand electronic signature service, which provides online display, certified delivery, acknowledgement, electronic signature, and storage services for eDocuments via the Internet.

"eDocument(s)" means a document(s) in electronic form sent to the Service by Customer via DocuSign Signature in order to be signed by one or several Signer(s). The eDocument may also be signed by other signatories with a different level of security for the signature (basic, advanced or qualified).

"eIDAS" means EU Regulation No. 910/2014.

"ID Check for AES" (or "Service") means the DocuSign ID Check for AES service which provides (i) Advanced Electronic Signatures, (ii) the RA online interface and (iii) evidence storage services. The Service is accessible via DocuSign Signature.

"Major Security Incident" means activity on or affecting: (i) the Service and/or (ii) Signer's data, that is likely to result in a loss of integrity, confidentiality, availability, and/or proof in the Service, including the Signer identification operation made by CA, Signer revocation requests made by Customer, personal data storage in DocuSign Signature, and the DocuSign Signature and Signer signing operation.

"Private Key" means a mathematical key, associated to the Public Key, that is secret, uniquely contained within a hardware security module (HSM), and remotely activated by the Signer to sign eDocuments. For the purposes of this GTU, the Private Keys are generated for only the purpose of a single Transaction and are erased after the completion of such Transaction.

"Proof File(s)" means a file generated, signed and time stamped by DocuSign that contains information related to the authentication during the ID proofing made by the RA and the signature process, including a copy of the Signer's official ID document. A dedicated Proof File is created for each Transaction. Each Proof File is only available to DocuSign in its role as Trust Service Provider.

"Proof of DocuSign Signature Application" (or "Certificate of Completion" or "COC") means a file generated via DocuSign Signature that contains information about eDocument signing activity, including information about the Signer, the sender of the eDocument, and the unique identifier of the Transaction used to manage the eDocument. A dedicated COC associated to each eDocument, Signer, and sender is generated for the purpose of proving the validity of a Transaction. COCs are sealed by DocuSign, Inc.

"Registration Authority (or "RA") is DocuSign, the entity that registers requests for the issuance, renewal, and revocation of Certificates. The RA collects electronic copies of Signer's ID document to verify the name of the Signer and to constitute evidence of the Signer's identity. The RA interacts directly with the CA and uses DocuSign Signature to interact with the Signer.

"Registration Policy" means the procedures and rules defined and implemented by the Registration Authority in order to identify and authenticate Signers, to verify and store supporting documents for Signers' registration, and to register requests to issue, renew, and revoke Signer Certificates.

"Signer(s)" means any individual who signs eDocuments with the Service.

"Signer Information" means the personal data (including name, email address, mobile phone number, and copy of an official ID document) used to identify a Signer.

"Transaction(s)" means the performance of a signature process, defined by a set of eDocuments submitted for electronic signature, by one or more Signers via DocuSign Signature.

"Vulnerability" means a path in the Service, data or in the Customer system that may lead to a Major Security Incident.

2. PROCEDURE FOR REQUESTING CERTIFICATES VIA THE SERVICE

2.1 You are informed and You accept that DocuSign, following the execution of the ID proofing and Consent Protocol, generates on Your behalf an Advanced Electronic Signature on the eDocuments.

2.2 In accordance with standards set by the European Telecommunications Standards Institute (ETSI), You are informed of and you accept that:

(a) Your Signer Information is verified by the RA and then registered in DocuSign Signature;

(b) You may view an eDocument transmitted by Customer to You via DocuSign prior to signing such eDocument using the Consent Protocol;

(c) The RA shall verify the authenticity of Your official ID document against the Signer Information. Upon the verification of Your Signer Information, the RA shall present the Consent Protocol to You to enable You to continue with the signing process. You may accept or refuse to sign the eDocument and may accept or refuse this GTU via DocuSign Signature;

(d) A dedicated signing Private Key is uniquely generated and securely assigned to You for the duration of the transaction. The Private Key is generated, stored and destroyed upon the completion of the Transaction so that it cannot be used for any other Transaction. The Private Key is associated with a Certificate, generated by the CA, and contains your identity information;

(e) The CA shall generate and archive a Proof File which is only available to DocuSign in its role as Trust Service Provider. The Proof File shall contain:

- The reference of the eDocument (unique identifier) presented to the Signer before signature;
- The signature of the eDocument;
- The date and time of the signature operation;
- The Consent Protocol as executed between the Signer and the CA;
- Registration information used to run the Consent Protocol and to populate the Certificate;
- ID proofing result; and
- A copy of Your official ID, including the personal data contained on your official ID;

(f) DocuSign Signature builds and stores the COC. You can download the COC via DocuSign Signature;

(g) Once signed, the eDocument can be downloaded from DocuSign Signature by the Customer and Signer immediately after the signature process. In any case, You will receive an email after completion of the Transaction giving you access to the signed eDocuments and the COC.

3. CERTIFICATE OF ISSUANCE. You must verify the content of the information in the Certificate (including the "subject" field of the Certificate, which contains Your complete first and last name) which are presented to You through the Consent Protocol. In case of any problem with the Certificate content, You shall immediately cancel the signature operation and inform the Customer.

4. CERTIFICATE PUBLICATION. The Certificate is not published by the CA or the RA. The Certificate is contained in the signed eDocument.

5. CERTIFICATE PERIOD OF VALIDITY. Certificates shall be valid for ten (10) days. Said period shall begin on the date the Certificate is created by the CA. Upon expiry of this Certificate period of validity, the signatures of eDocuments may be verified with verification software, notably in order to verify that on the eDocument date of signature, the Certificate was valid at the moment of the signature.

6. EFFECTIVE DATE OF DURATION. The present GTU shall take effect from the Effective Date, coinciding with the Certificate request date and shall apply for the period of validity of the Certificate.

7. REVOCATION

7.1 Revocation Generally. In its capacity as CA, DocuSign enables Signer and/or Customer to report inaccurate Signer Information. These reports are revocation requests. If DocuSign receives an authenticated online revocation request through the Personal Certificate Revocation Request Form (as described in Section 7.2) from Customer within the first ten (10) days after a Certificate is issued, DocuSign shall add the Signer's Certificate to the Certificate Revocation List maintained and published by the CA.

Revocation information will always be available from the CA that publishes a CRL. In the event of the CA's end of life or the Service stopping with this CA or even in the event of a compromised CA key, a CRL will be generated and archived at DocuSign France. This CRL is published on the DocuSign France website until the TSP ends its activity. It is also published on the CRL distribution URL contained in the Certificate until the last Certificate issued by the CA expires.

7.2 Revocation at the Request of Signer. You shall submit a revocation request to the CA by submitting the Personal Certificate Revocation Request Form (located at https://docusign.fr/revocation) if:

(a) There are any inaccuracies in Your Signer Information; or

(b) The Certificate corresponding to the Private Key has been compromised or is suspected to be compromised.

In order to submit a revocation request, you will need the unique identifier of the eDocument as well as access to the same email address used during the signature process (refer to Signer Information) in order to receive temporary code sent by DocuSign France to authenticate You for the revocation operation.

7.3 Revocation by DocuSign. In its capacity as CA, DocuSign shall revoke a Certificate if:

(a) The CA is revoked;

(b) Signer or RA fails to comply with their obligations to verify the accuracy of Signer Information;

(c) The Certificate corresponding to the Private Key has been or is suspected to be lost or compromised; or

(d) For any other legitimate reason as determined by the CA.

8. OBLIGATIONS OF SIGNER. By accepting this GTU, You acknowledge and agree to:

(a) Ensure the security and confidentiality of any temporary code You receive in order to access or use the Service or to revoke Your Certificate;

(b) If applicable, ensure the security and confidentiality of any authentication credential provided by the Customer in order for You to use the Service;

(c) If applicable, ensure the security and confidentiality of any links you receive to access the Service;

(d) Verify the authenticity and accuracy of the information of Signer identity that is presented to You through the Consent Protocol and, for at least ten (10) days after signing any eDocument, retain sole access and control of your email address;

(e) Immediately cancel the signature operation within the Service and inform the RA via Customer if there are any inaccuracies in your Signer Information;

(f) Promptly request the CA via the Personal Certificate Revocation Request (as described in Section 7.2) to revoke a Certificate in the event of suspected or actual theft, unauthorized disclosure, or compromise of any documents or information used to authenticate your Signer Information, including your mobile phone number and official ID document;

(g) Inform the RA via Customer of any change to Your Signer Information;

(h) Provide a valid copy of Your official ID document when requested within the Service; and

(i) Record the signed eDocument and signed GTUs to have access to the unique identifier in case You need to revoke Your Certificate.

9. LIMITATIONS OF LIABILITY. DocuSign's sole liability to You shall be for direct and foreseeable damages in case of breach of its statutory obligations. Any other liability arising from or related to the use of the Service, including without limitation any liability related to the use of the Public Keys, Private Keys, the Certificates and/or the eDocuments contents shall fall to the Customer, and is subject to the terms agreed between You and the Customer.

10. FORCE MAJEURE. Neither party shall be liable for any non-fulfilment or delay in the fulfilment of one or more obligations under this GTU due to a case of force majeure as defined under Article 1218 of the French Civil Code.

11. PROTECTION OF PERSONAL DATA. The personal data collected from Signer by DocuSign, acting as CA and RA, is processed by DocuSign for the sole purposes of (a) authentication and identification of the Signer, (b) creation of the Signer Information filled in the Certificate, (c) authentication of the Signer during the Consent Protocol, and (d) revocation of the Certificate. Your personal data is stored for the sole purposes of (i) creation of the Signer Information filled in the Certificate, (ii) authentication of the Signer during Consent Protocol, and (iii) fulfilling DocuSign’s obligations as a CA, including creation of the Proof File.

DocuSign, acting as CA and RA, processes and stores Your personal data in accordance with the applicable French and European law and regulations regarding personal data and privacy protection, including eIDAS. You, as Signer, have the right to access and rectify your personal data and to oppose to the processing of your personal data on legitimate grounds in accordance with DocuSign’s Privacy Policy.

Any opposition to the retention of Your personal data shall prevent the issuance of a Certificate. Your personal data may also be retained by the Customer. The Customer defines its own personal data retention period, depending on the legal requirements regarding the eDocuments.

12. INTELLECTUAL PROPERTY. You acknowledge and agree that DocuSign shall retain all intellectual property rights (patents, registered trademarks and other rights) for the elements comprising the Service as well as the documentation, concepts, techniques, inventions, processes, software, or work performed in connection with the Certificates and related services made available by DocuSign, irrespective of the form, programming language,

program medium, or language used. This GTU does not confer to You any intellectual property right with regard to the Certificates, the Service, or any related services.

13. GOVERNING LAW

13.1 If You are acting for professional purposes, the following paragraph shall apply to You: This GTU 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 this GTU 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 GTU 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: this GTU 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 GTU or its subject matter or formation.

14. CUSTOMER SUPPORT. The Customer is responsible to provide You the technical support which could be necessary and to deal with any request in accordance with the support service terms and conditions agreed between the Customer and DocuSign.

15. WAIVER. The waiver by either party of any breach of any provision of this GTU does not waive any other breach. The failure of any party to insist on strict performance of any covenant or obligation in accordance with this GTU 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 this GTU.

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

17. MODIFICATION OF GTU. DocuSign shall have the right to change, modify, or amend any portion of this GTU at any time by posting sufficient prior notification on the DocuSign website or otherwise communicating the notification to You to the sole extent that it implies a substantial modification of the GTU. The changes will become effective after expiration of the notification period, and shall be deemed accepted by You if You continue using the Service after such period. In the event that You do not agree with any such modification, You shall discontinue Your use of DocuSign ID Check for AES.

18. ENTIRE AGREEMENT. This GTU, which includes the language and paragraphs preceding Section 1, is the final, complete, and exclusive expression of the agreement between these parties regarding ID Check for AES provided under this GTU. This GTU supersedes, and the parties disclaim any reliance on, all previous oral and written communications (including any confidentiality agreements pertaining to ID Check for AES under this GTU, 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.

19. LANGUAGES AND TRANSLATION. DocuSign may provide translations of this GTU or other terms or policies. Translations are provided for informational purposes and if there is an inconsistency or conflict between a translation and the French version, the French version will control.