DOCUSIGN TERMS OF USE:
ID CHECK REMOTE FOR QES

Updated: April 15, 2022

The purpose of these Terms of Use ("GTU") is to govern: (i) your, the Signer's ("You", "Your", or "Signer"), use of the ID Check RemoteService for QES ("ID Check Remote for QES"); (ii) the associated Certificate, defined below, delivered by DocuSign; and (iii) and Your and Customer's obligations.

You agree to be bound by the terms of these GTU as of the date of Your accepting this GTU ("Effective Date") and represent You have the authority to bind any party on whose behalf you are signing. Certificates are generated and managed in the context of the online qualified electronic signature service provided by DocuSign to the Customer.

1. Definitions

"Certificate(s)" means the Certificate generated by the CA via the Service for a Signer, which attests the unique link between the Signer's name as presented on Signer's ID, Certificate and an Electronic Signature Creation Data. In this case, the term "Certificate" means the qualified certificate for electronic signature, as defined in Article 3-15 of eIDAS, generated by DocuSign to the benefit of a Signer to create a qualified electronic signature.

"Certification Authority" (or "CA") is DocuSign, the authority that generates Certificates and manages the Certificate lifecycle (issuance, renewal, revocation) and associated Electronic Signature Creation Data on the request of the Registration Authority, in accordance with the rules and practices defined in its Certificate Policy(ies). The technical name of the CA contained in the EU trust list is "DocuSign Premium Cloud Signing CA - SI1".

"Certificate Policy(ies)" (or "CP") means the set of rules published by the CA. A Certificate Policy describes the general characteristics of the Certificates and Electronic Signature Creation Data that it issues and the roles of the CA, the RA, the Signer and relying parties. The Certificate Policy of DocuSign and its (their) successive update(s) is designated as 1.3.6.1.4.1.22234.2.14.3.31 and is available at: https://www.docusign.fr/societe/certification-policies.

"Consent Protocol" means the procedure within the Service accessible via DocuSign Signature by which You consent to receive a Certificate with the Signer's name, email and mobile phone number (and other fields designed by DocuSign), to accept signing the eDocument via the Service, and to accept signing 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 any content stored in electronic form, in particular text or sound, visual or audiovisual recording.

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

“ID Check Remote for QES” (or “Service”) means the service which provides (i) qualified electronic signature under the meaning of European Regulation 910/2014, (ii) RA online interface, and (iii) evidence storage services. The QES Service is accessible via DocuSign Signature.

“Electronic Signature Creation Data” means a mathematical key, associated to the Certificate, that is secret, uniquely contained within a certified remote Qualified Signature Creation Device, as defined in Article 3-23 of eIDAS, and remotely activated by Signer to sign eDocuments as permitted under the GTU.

“Proof File(s)” means a file generated, signed and time-stamped by DocuSign that contains the below-listed information related to the Signer identification and the signature generated by the Service. Specifically, the Proof File contains:

- A reference to the eDocument and GTU presented to the Signer before signature;
- The signature of the eDocument and signed GTU including the Certificate;
- The signed 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
- Registration information used to run the Consent Protocol and to populate the Certificate.

Each Proof File is only used by DocuSign in its role as Trust Service Provider as defined in eIDAS regulation. Customers may request an electronic copy of the Proof File upon request and as outlined in DocuSign’s Certificate Policy.

“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, sender of the eDocument, and 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. and made available to the Customer.

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

“Registration Authority” (or “RA”) means the entity in charge of registering requests for issuance, renewal, and revocation of Certificates. The RA collects the signed RIVR from the RIVSP in order 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 RIVSP and Signer. For the purposes herein, the RA is DocuSign.

“Remote Identity Verification Service Provider” (or “RIVSP”) means the third party service provider responsible for acquiring and verifying Signer’s facial image and Signer’s ID document in order to identify You, producing the evidence file and sending the Result of the Remote Identity Verification to the RA. The RVISP is certified by ANSSI (the French supervisory body according eIDAS).

“Remote Identity Verification Result (“RIVR”)” means the signed information sent by the RIVSP to the RA, 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 RA (name, 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).“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).

2. PROCEDURE FOR REQUESTING CERTIFICATES VIA THE QES SERVICE

2.1 You are informed and You accept that DocuSign, following the execution of the ID and Signer verification and Consent Protocol, generates on Your behalf a Qualified Signature on the eDocuments and GTU.

2.2 In accordance with standards set by the European Telecommunications Standards Institute (refer to here: https://www.etsi.org/) and RIVSP standard (https://www.ssi.gouv.fr/en/actualite/publication-of-the-requirement-rule-set-for-remote-identity-verification-service-providers/), You are informed of and You accept that:

A. Before You sign, You will be identified by RIVSP using interaction defined by the RIVSP and requiring the Signer’s ID and liveness detection of Signer’s facial image.

B. The RIVSP, after identifying You and collecting the Signer’s name extracted from Your ID and information from Your ID, performs a manual review of Your identification and creates the RIVR.

C. The RA shall verify the authenticity of the RIVR. Upon the verification of the RIVR and the successful result given by the RIVSP, the RA will use Your email, mobile phone number and name from the RIVR and invite You by email or SMS to connect to DocuSign Signature and present You with the Consent Protocol to You to enable You to continue with the signing process. You may accept or refuse to sign the eDocument and this GTU via DocuSign Signature. To confirm Your signing, You will be required to enter a temporary code in the Consent Protocol transmitted by the CA to Your registered mobile phone number.

D. Dedicated signing Electronic Signature Creation Data is uniquely generated and securely assigned to You for the duration of the eDocument and GTU signature transaction. The Electronic Signature Creation Data is generated, stored and destroyed upon the completion of the signature transaction so that it cannot be used for any other signature transaction.

E. The CA shall generate and archive a Proof File and store it in a dedicated electronic vault by a qualified preservation service provider located in France. A dedicated Proof File is created for each Transaction.

F. Once signed, the GTU will be immediately transmitted to You via the email indicated in the Consent Protocol after the signature process.

3. CERTIFICATE ISSUANCE. You must verify the content of the information to be set 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. At no cost, DocuSign will provide you with access to verify the validity status of the Certificate.

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

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 and GTU may be verified with verification software, notably in order to verify that on the eDocument and GTU date of signature, the Certificate was valid at the moment of the signature. Certificate contains the internet link where to find and use validation service of Certificate provided at no cost by DocuSign.

6. EFFECTIVE DATE AND 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 to report a potential or actual incorrect Signer's name, email and/or mobile phone number to the CA. These reports are revocation requests. If Signer submits an authenticated online revocation request through the Personal Certificate Revocation Request Form (as described in Section 7.2) to the CA in the first ten (10) days after a Certificate is issued, DocuSign, shall add the Signer's Certificate to the certificate revocation list (CRL), signed and published by CA, within twenty-four (24) hours of receiving such request from the Signer.

Revocation information will always be available from the CA that publishes a CRL. In the event of end of the CA's life or the Service stopping with this CA or even in the event of a compromised CA key, a last 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. Signer shall submit a revocation request to the CA by submitting the Certificate revocation application form (located at https://docusign.fr/revocation) if:

(a) There are any inaccuracies in Your Signer's email, mobile phone number and/or name;
(b) The Electronic Signature Creation Data corresponding to the Certificate has been compromised or is suspected to be compromised;
(c) The RIVSP did not conduct facial image verification of You; or
(d) The RIVSP did not request You to present Your official ID document.

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 section 2.2 above) in order to receive temporary code sent by DocuSign France to authenticate You for the revocation operation.

The certificate will be revoked within twenty-four (24) hours from the time the request is processed following successful authentication of the Signatory with the temporary code filled in the online revocation interface.

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

(a) The CA is revoked;
(b) Signer, RIVSP or RA fails to comply with their obligations;
(c) The Electronic Signature Creation Data corresponding to the Certificate 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 which You shall use to sign (received on Your mobile phone number) the eDocument or to revoke Your Certificate (received on Your email);
(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 about the Signer's name, email and mobile phone number 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 Customer if there are any inaccuracies in your Signer's name, email and mobile phone number;

(f) Promptly request the CA via online revocation interface (refer to section 7.2 above) to revoke a Certificate in the event of suspected or actual theft, unauthorized disclosure, or compromise of any documents or information used to identify You with RIVSP, including your mobile phone number and official ID document;
(g) Inform the Customer of any change to Your Signer's name, email and/or mobile phone number;
(h) Provide a valid copy of Your official ID document when requested in the RIVSP online interface;
(i) Record the signed eDocument and signed GTUto have access to the unique identifier in case You need to revoke Your Certificate; and
(j) As provided in Section 11 below (Protection of Personal Data), You Grant DocuSign permission to collect, use, and share your name, email, phone, ID, photo and data in the RIVR and share it with the third party RISVP provider for purposes of the Service and to improve our products.

9. LIMITATION OF LIABILITY. SUBJECT TO ANY CONFLICT WITH WITH ARTICLE 13 OF EIDAS, DOCUSIGN'S SOLE LIABILITY TO YOU FOR USE OF OUR SERVICES, INCLUDING ID CHECK RIVSP FOR QES, SHALL BE GOVERNED BY SECTION 11 (LIMITATIONS OF LIABILITY) OF DOCUSIGN'S SITES AND SERVICES TERMS AND CONDITIONS (https://www.docusign.com/company/terms-and-conditions/web).

10. FORCE MAJEURE. Neither party shall be liable for any non-fulfilment or delay in the fulfillment 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 (only contained in the RIVR) and RIVSP, acting as CA and RA, is processed by DocuSign and RIVSP for the sole purposes of (a) authentication and identification of the Signer, (b) creation of the Signer's name 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's name filled in the Certificate, (ii) authentication of the Signer during Consent Protocol, (iii) revocation of the Certificate and (iv) construction of Proof File used as proof for DocuSign in case of; audit as defined in eIDAS regulation and trial, dispute or legal inquiry. The Proof file is stored in a qualified archive service provider and by DocuSign France in compliance with eIDAS security rules.

By consenting to these GTU, You agree that the RA and the CA shall retain a Proof File containing your personal data and the RIVSP shall retain, according to the RIVSP I data privacy policy, Your personal data for a period of seven (7) years after the Certificate expires. During this period of time Your personal data can't be deleted or modified for any reason.DocuSign, acting as CA and RA, processes and stores Your personal data in accordance with the applicable laws and regulations governing it as a CA and Trust Service Provider. These laws and regulations require us to store your personal information for defined retention periods as set out in our data retention policy and information handling standards (refer to https://www.docusign.com/company/privacy-policy).

Your personal data contained in COC and in Customer’s account in DocuSign Signature platform (such as Signer’s ID photo, Signer’s facial image, gender and other Signer’s data contained in the RIVR due to ID Verification service) may also be retained by the Customer. The Customer defines its own personal data retention period.

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. Customer Support is available from Monday to Friday, from 9am to 6pm, CEST working days in France, except on legal holidays. It can be reached directly by phone (+33 975181331) or on our Support page.

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 ID Check RIVSP for QES.

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 the ID Check RIVSP for QES service 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 RIVSP for QES 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 TRANSLATIONS. 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.