ConditionConditions Générales d'Utilisation du service Trust and Sign (niveau LCP)

1 CONTENU

L'objectif des présentes Conditions Générales d'Utilisation (ci-après dénommées **CGU**) est de définir les conditions juridiques relatives à l'acquisition et l'utilisation des Certificats DocuSign France ainsi que les obligations correspondantes de DocuSign France, de l'autorité d'enregistrement (ci-après dénommée 'AE'), du Client ainsi que de l'Utilisateur. Les certificats des Utilisateurs sont fournis et gérés par l'intermédiaire du service en ligne de signature électronique avancée de DocuSign France. Ce Certificat associé au service de DocuSign France de signature permet à l'Utilisateur de signer électroniquement le(s) Document(s) avec un niveau avancé conformément à l'article 26 du règlement européen E N° 910/2014 (Règlement eIDAS) et à la norme ETSI 319 411-1 (LCP) pour le niveau de sécurité du Certificat.

2 DÉFINITIONS

Autorité de certification (ou AC) : désigne l'entité qui émet les Certificats et gère le cycle de vie des Certificats (émission, renouvellement, révocation) et des Clés Publiques et Privées à la demande de l'Autorité d'Enregistrement, conformément aux règles et pratiques définies dans la Politique de Certification. Dans le cadre des présentes CGU, l'AC est DocuSign France.

Autorité d'enregistrement (ou AE) : désigne l'entité approuvée par l'AC, et contractuellement liée à l'AC, pour enregistrer les demandes d'émission, de renouvellement et de révocation des Certificats, les valider ou les rejeter et ce, en application de ses règles et ses pratiques (appelé Politique d'Enregistrement) approuvées par l'AC conformément à la Politique de Certification de l'AC. Dans le cadre des présentes CGU, l'AE est NETHEOS.

Certificat : désigne un fichier électronique délivré par l'AC et attestant du lien entre l'Iidentité de l'Utilisateur et la Clé Publique associée à la Clé Privée de l'Utilisateur.

Clef privée : Clef mathématique secrète et unique contenue sur un appareil et pouvant être activée à distance par le souscripteur pour signer des documents électroniques. DocuSign France est en charge de la génération, protection et destruction des clés privées, dans une ressource cryptographique matérielle certifiée FIPS 140 – 2 level 3, utilisées par les Utilisateurs dans le cadre des présentes.

Clef publique : Une clef mathématique devant être publiée et utilisée pour la mise en place d'un protocole cryptographique permettant de vérifier la signature d'un document. DocuSign France est en charge de la génération des clés publiques, dans une ressource cryptographique matérielle certifiée FIPS 140 – 2 level 3, utilisées par les Utilisateurs dans le cadre des présentes.

Client : Entité légale proposant la signature d'un ou plusieurs Document(s) à un Utilisateur.

Conditions générales d'utilisation (CGU) : désigne les présentes conditions juridiques relatives à l'utilisation du Service.

Document(s) électronique(s) : Document au format numérique créé par le Client et présenté pour signature par l'Utilisateur. Le Document électronique peut être signé par le client en tant que personne juridique à l'aide d'un cachet électronique.

Fichier(s) de preuve : désigne un fichier électronique créé, signé et horodaté par DocuSign France contenant toutes les informations pertinentes relatives ; au receuil du consentement de l'Utilisateur, aux informations transmises par l'AE et à l'activation du processus de signature du Document. Un fichier de preuve dédié est généré pour chaque demande de l'AE auprès de l'AC afin de faire la preuve en cas de litige sur le processuss de signature et d'émission de Certificat.

Identité de l'Utilisateur : L'identité élaborée à partir des données collectées par l'AE sur l'Utilisateur ainsi que les données définies par l'AE. Cette identité sera utilisée pour authentifier une personne physique à l'aide de ses noms et prénoms telque porté sur son titre d'identité officiel (passeport, carte d'identité ou carte de séjour) et sera inscrite dans le Certificat.

Liste de Certificat Révoqué (LCR) : Liste des certificats invalides révoqués expiré ou pas. La LCR

est publiée régulièrement et signée numériquement par l'AC.

Politique d'Enregistrement (PE) : désigne l'ensemble de règles publiées par l'AE décrivant les obligations et rôles de l'ensemble des entités et participants impliqués dans la procédure d'enregistrement. La version applicable de la PE est celle en vigueur à la date d'initialisation du Service. Elle peut être consultée sur le site Internet de l'Autorité d'Enregistrement à l'adresse suivante : https://www.netheos.com/politique_enregistrement_certification/082019_C1_DEM_v1.1_politique_d_enregistrement_et_declaration_des_pratiques_d_enregistrement.pdf.

Politique(s) de certification (PC) : désigne l'ensemble de règles identifiées par un OID (Object Identifier) et publiées par l'Autorité de Certification, décrivant les caractéristiques générales des Certificats qu'elle émet. Une Politique de Certification décrit les obligations et rôles de l'ensemble des entités et participants impliqués dans le cycle de vie global d'un Certificat.

La Politique de Certification utilisée à la date de signature des présentes CGU est identifiée par l'OID 1.3.6.1.4.1.22234.2.14.3.32 et est complétée par la Politique d'Enregistrement.

La version applicable de la Politique de Certification est celle en vigueur à la date d'initialisation du Service. Elle peut être consultée sur le site Internet de l'Autorité de Certification : https://www.docusign.fr/societe/certification-policies.

Protocole de consentement : désigne la procédure suivant laquelle le consentement du Signataire à recevoir un Certificat avec une Identité Signataire et à signer un Document électronique via le Service est collecté via l'application de DocuSign France.

Utilisateur(s) (ou Signataires) : désigne la personne physique pour laquelle le Client crée les Documents et qui utilise le Service pour signer électroniquement lesdits Documents. L'Utilisateur peut utiliser le Service uniquement pour signer les Documents présentés par le Client.

Service : Tous les services réalisés par DocuSign France et Netheos conformément aux CGU, notamment pour permettre l'utilisation du Certificat et de la Clef privée qui y est associée, la mise en œuvre du Protocole de consentement et l'enreigistrement de l'Utilisateur.

3 PROCÉDURE DE DEMANDE DE CERTIFICAT VIA LE SERVICE

L'Utilisateur est informé et accepte expressément le fait qu'afin d'apposer sa signature électronique sur les Documents présentés par le Client, le Client utilise les services d'enregistrement offerts par Netheos et l'application de DocuSign France pour la signature électroniqe.

Dans ce cadre :

- Le Client élabore et transmet le(s) Document(s) à faire signer par l'Utilisateur ainsi que le(s) nom(s) (au moins le premier tel qu'inscrit sur sa pièce d'identité officielle) et prénom(s), adresse de courrier électronqiue et numréo de téléphone portable de l'Utilisateur qui doit signer à l'AE ;
- L'Utilisateur doit ensuite télécharger la copie électronique de sa pièce d'identité officielle sécurisée (passeport, carte d'identité ou titre de séjour) en cours de validité dans l'interface de l'AE ;
- L'AE vérifie l'identité de l'Utilisateur en comparant le(s) nom(s) et prénom(s) transmis par le Client et ceux contenu dans la pièce d'identié transmise par l'Utilisateur. L'AE vérifie aussi les caractèristiques de la pièce d'identité afin de s'assurer de la vraisssamblance du titre d'identité ;
- Si la vérification de l'AE n'est concluante alors, l'AE rejette la demande. Si la vérification est concluante, alors l'AE transmet à l'AC le premier nom et prénom de l'Utilisateur, le(s) document(s) à signer et le numéro de téléphone de l'Utilisateur. L'AE constitue son ensemble de preuve lié à cette opération constituée des données personnelles de l'Utilisateur (y compris la copie de la pièce d'identité et de leur vérification) ;
- L'Utilisateur entre alors en communication direct avec l'AC qui met en œuvre le

Protocole de consentement qui permet de présenter le(s) Document(s), le premier prénom et nom de l'Utilisateur, les CGU en cliquant sur le lien internet prévu à cet effet et le numéro de téléphone de l'Utilisateur. L'AC transmet un code temporaire dédié à l'Utilisateur sur le numéro de téléphone portable de l'Utilisateur ;

- L'Utilisateur est invité à valider dans l'interface du Protocole de consentement l'ensemble des informations et à signer en cliquant sur la ou les case(s) à cocher et en entrant le code temporaire. Si l'Utilisateur ne souahite pas signer ou constate une erreur dans les données présentées dans le Protocole de consentement alors, il abandonne la signature en cliquant sur un lien prévu à cet affet dans le Protocole de consentement ;
- Si l'Utilisateur choisit de signer, alors l'AC génère une Clé privée, une Clé publique et un Certificat associé et signe le(s) Document(s) à l'aide de cette Clé privée. La Clé privée est immédiatement détruite après l'opération de signature afin qu'elle ne puisse pas être réutilisée ;
- Suite à la fin de l'opération de signature, l'AE transmet à l'AC l'ensemble des journaux créé suite à l'opération de vérification de l'identité de l'Utilisateur (ensemble des vérifications et de la ou les pièce(s) d'identité de l'Utilisateur) ;
- L'AC génère un Fichier de preuve qui contient les données transmises par l'AE ;
- L'AC pousse le Fichier de preuve dans un service d'archivage électronique accessible par le Client.

4 ACCEPTATION DU CERTIFICAT

L'Utilisateur est responsable de la vérification du contenu du certificat (en particulier concernant le champ 'sujet' du certificat contenant le prénom et nom complets de l'Utilisateur). L'Utilisateur et le Client disposent d'un délai maximum de huit (8) jours à partir de la date de délivrance du certificat pour rejeter le contenu du Certificat et déposer une demande de révocation auprès de l'AE. Passé ce délai de huit jours, le Certificat sera réputé accepté par l'Utilisateur et ne pourra plus être révoqué à sa demande.

5 PUBLICATION DU CERTIFICAT

L'AC et l'AE ne peuvent publier le Certificat. Le Certificat est inclus dans le(s) Document(s) ainsi que dans le Fichier de preuve.

6 VALIDITÉ DU CERTIFICAT

Les Certificats sont valides sur une période maximale de dix (10) jours. La période susmentionnée débute à la date de génération du Certificat par l'AC. Une fois la période de validité du Certificat écoulée, la ou les signature(s) du ou des Document(s) peuvent être vérifiées avec les logiciels de vérification mentionnés par le Client (généralement Adobe Reader), notamment pour vérifier que les Documents ont été signés électroniquement avec un Certificat valide délivré par l'AC au moment de la signature.

7 CONDITIONS DE RÉVOCATION DU CERTIFICAT

L'Utilisateur concerné est toujours informé de la révocation du Certificat par l'AE.

7.1 Révocation à l'initiative de l'Utilisateur ou du Client

L'Utilisateur et le Client peuvent révoquer le Certificat en soumettant une demande auprès de l'AE. Cette demande peut être soumise via l'adresse de courrier électronique : revocation@netheos.net
Dans les cas suivants, l'Utilisateur et le Client peuvent procéder à une demande de révocation :

- Les informations de l'Utilisateur figurant dans le Certificat sont incorrectes ;
- L'Utilisateur pense que le code temporaire a été volé ou que son téléphone portable est piraté ;
- L'AE n'a pas respecté sa Politique d'Enregistrement.

La demande de révocation est transmise par courrier électronique à l'AE et doit contenir les informations suivantes :

- Nom et Prénom de l'Utilisateur ;
- Date de naissance ;

- Adresse de courrier électronique de l'Utilisateur.

L'AE est en charge d'authentifier les demandes de révocation et de les valider avant de les transmettre à l'AC. Ces demandes sont traitées du lundi au vendredi entre 09h00 et 18h00.

Le Certificat sera révoqué sous vingt-quatre (24) heures à compter du moment où la demande sera prise en charge par l'AE.

7.2 Révocation à l'initiative de l'AC

Dans les circonstances suivantes, le Certificat sera révoqué par l'AC avec effet immédiat :

- L'AC est révoquée ;
- L'Utilisateur ou l'AE n'a pas respecté ses obligations et les règles de sécurité définies dans la Politique de Certification et la Politique d'Enregistrement et les CGU ;
- La Clé privée correspondant au Certificat a été perdue ou compromise, ou est soupçonnée de l'être (par exemple le Signataire a perdu son téléphone et sa pièce d'identité).

7.3 Révocation à l'initiative de l'AE

Dans les circonstances suivantes, le Certificat sera révoqué par l'AE avec effet immédiat :

- Les informations de l'Utilisateur figurant dans le Certificat sont incorrectes ;
- L'AE n'a pas respecté sa Politique d'Enregistrement.

Les informations de révocation seront toujours disponibles auprès de l'AC qui publie une CRL. En cas de fin de vie de l'AC ou d'arrêt du Service avec cette AC ou y compris en cas de compromission de clé d'AC, une dernière CRL est générée et archivée chez DocuSign France. Cette dernière CRL est publiée sur le site internet de DocuSign France jusqu'à expiration du TSP et sur l'URL de distribution de la CRL, contenue dans le Certificat, jusqu'à expiration du dernier Certificat émis par l'AC.

8 CONDITIONS ET PÉRIODE DE VALIDITÉ

Les présentes CGU sont considérées comme étant valides et acceptée à partir du moment où l'Utilisateur coche la case prévue à cet effet dans le page de Protocole de Consentement.

Les présentes CGU s'appliquent pendant une période équivalente au cycle de vie des Certificats émis au profit de l'Utilisateur et cessent de s'appliquer à la date de fin de validité desdits Certificats.

9 OBLIGATIONS DE L'UTILISATEUR

En acceptant d'utiliser ce service, l'Utilisateur accepte de respecter les modalités les présentes CGU et de :

- Fournir au Client et à l'AE des informations exactes et authentiques ;
- Protéger la sécurité et la confidentialité du code temporaire transmis par l'AC et reçu par SMS utilisé pour signer le(s) Document(s). Ce code doit étre détruit par l'Utilisateur après avoir procédé à la signature électronique ;
- Vérifier le contenu du Certificat et alerter le Client ou l'AE si le Certificat n'est pas correctement rempli ;
- Vérifier l'authenticité et l'exactitude des informations à indiquer dans le Certificat et à utiliser pour recevoir le code temporaire, telles qu'elles sont présentées lors du Protocole de Consentement ;
- Demander dans les meilleurs délais la révocation du Certificat à l'AE, si besoin est ;
- Aviser dans les plus brefs délais, l'AE de tout changement concernant les moyens d'authentification utilisés par l'AE et l'AC (numéro de téléphone et adresse de courrier électronique).

10 RESPONSABILITÉ

L'AC et l'AE ne peuvent être tenue responsable de tout dommage indirect ou imprévisible subi par le Souscripteur, tel qu'un préjudice financier ou commercial, une perte de bénéfices, un manque à gagner, une perte de clients, des troubles commerciaux, une perte de revenus ou la perte de

données causée par les, ou résultant des présentes CGU ou se rapportant à l'utilisation des Certificats.

Dans l'hypothèse où la responsabilité de l'AC devrait être engagée, il est expressément convenu que DocuSign France sera tenue d'indemniser tout préjudice direct, certain et immédiat.

Dans l'hypothèse où la responsabilité de l'AE devrait être engagée, il est expressément convenu que l'AE sera tenue d'indemniser tout préjudice direct, certain et immédiat.

L'AE et DocuSign France n'acceptent aucune responsabilité en ce qui concerne l'utilisation des Certificats ou de la Clé Privée associée, émise par le biais du Service, à des conditions, et pour des finalités autres que celles prévues par les présentes CGU, à savoir pour vérifier la signature électronique apposée sur les documents électroniques par le biais du Service.

Au regard du fait que ni l'AE ni l'AC DocuSign France n'a connaissance du contenu ou de la portée juridique des Documents, l'AE et l'AC ne peuvent être tenues responsable des conséqences juridiques de la signature des Documents et de leurs usages.

L'AE et l'AC ne sont pas en charge ni responsables de la qualité de la connexion Internet ou des conséquences d'un retard ou d'une perte lors de la transmission des courriers électronique et SMS, ou en ce qui concerne un retard, une altération ou toute autre erreur survenant lors de la transmission d'une télécommunication dans le cadre des présentes CGU. En outre, il est convenu que ni l'AE ou l'AC ne pourra être tenue responsable au titre d'un quelconque défaut de fonctionnement affectant le poste de travail de l'Utilisateur ni d'un usage détourné du Protocole de consentement ou de l'interface d'enregistrement de l'AE. De la même manière, la responsabilité de l'AE et de l'AC ne couvre pas le bon fonctionnement (panne, erreur, incompatibilité, etc.) du matériel informatique, des logiciels et de l'environnement de l'Utilisateur.

L'AC et l'AE ne pourront être tenue responsable et n'assume aucune responsabilité en ce qui concerne tout retard dans l'exécution des obligations ou toute inexécution des obligations découlant des présentes CGU lorsque les circonstances donnant lieu à ce retard ou cette inexécution résultent d'un cas de force majeure défini à l'Article 11 ci-dessous.

11 CAS DE FORCE MAJEURE

L'AC et l'AE ne peuvent être tenues responsables du manquement ou du retard dans l'exécution d'une ou de plusieurs obligations conformément aux présentes CGU en cas de force majeure, de circonstances exceptionnelles ou échappant à tout contrôle. Les cas de force majeure ou circonstances exceptionnelles sont celles retenues par la loi française et les tribunaux français.

12 PROTECTION DES DONNÉES PERSONNELLES

Conformément à loi française et européenne, l'Utilisateur est informé que les données personnelles collectées, à savoir sa pièce d'identité et toutes les données qu'elle contient, son adresse de courrier électronique et son numéro de téléphone, par l'AE et l'AC et le Client au cours du processus de gestion des Certificats seront traitées par l'AE pour :

(i) permettre à l'AE d'authentifier et d'identifier l'Utilisateur, (ii) de réaliser les vérifications nécessaires pour la délivrance ou le cas échéant la révocation des Certificats, (iii) de créer une Identité Signataire dans le Certificat, (iv) d'authentifier l'Utilisateur lors du Protocole de Consentement et (v) de consitituer des preuves des opérations d'authentification et de génération réalisées par l'AE et l'AC. L'AC et l'AE respectent la législation européenne relative à la protection des données personnelles. L'Utilisateur est informé que l'AE utilise les données à caractères personnelles contenues dans la pièce d'identité et celle transmises par le Client (nom et prénom de l'utilisateur) de manière automatisée afin de vérifier l'identité de l'Utilisateur et d'autoriser la demande de signature et donc la demande de génération de Certificat.

Ses données personnelles sont conservées par l'AE et l'AC à des fins de preuves conformément aux exigences eIDAS transposées par l'ANSSI et l'ETSI 319 411-1 (LCP). Ses données personnelles sont aussi conservées par le Client pour ses propres besoins légitimes. L'AE peut être contacté sur ces

sujet à cil@nethoes.net. L'AC peut être contacté sur ces sujets en passant par l'AE. Seules les personnes autorisées par le Client, l'AE et l'AC peuvent accéder aux données personnelles. L'Utilisateur est informé qu'il peut exercer ses droits auprès de l'AE et de l'AC suivant les modalités décrites dans ce paragraphe en contactant l'AE ou l'AC. Le traitement effectué sur les données personnelles par le Client est de sa seule responsabilité. L'Utilisateur peut contacter le Client suivant les modalités définies et communiqués auprès de l'Utilisateur par le Client. Au sein de de l'AE et de l'AC, seul un groupe restreint de personnes autorisées peuvent avoir accès à ces données uniquement aux fins de la gestion des éléments de preuve et de la résolution des incidents.

Toute objection au stockage des données personnelles empêche la délivrance d'un Certificat. Cette objection se manisfeste par le refus de signer dans la page de Protocole de Consentement. En ce cas, les données personnelles du Signataire sont conservées pendant 6 mois maximum par l'AE Seulement et ensuite détruites. En acceptant les CGU en cochant la case prévue à cet effet dans la page de Protocole de consentement, l'Utilisateur accepte que l'AE conserve les informations d'enregistrement sur une période de dix (10) ans, que l'AC conserve les Certificats sur une période de sept (7) ans minimums à compter de la date d'expiration du Certificat. Le Client peut les conserver plus longtemps en fonction de ses besoins métiers. L'Utilisateur est informé que seul le Client peut lui communiquer la durée de conservation de ses données personnelles. De même, le droit de rectification n'est possible qu'en utilisant la procédure de revocation. Toutes les données personnelles collectées et ayant permis de générer un Certificat ne peuvent être détruites et sont obligatoirement conservées pendant une durée définie ci-dessous et ensuite détruite à l'expiration de cette durée en fonction des règles suivantes de conservation par :

- L'AC (Certificat, potentiellement l'adresse IP de l'Utiilsateur) pour une durée adéquate, en fonction des exigences légales et réglementaires, et notamment afin d'assurer la continuité du Service et d'apporter les éléments de preuve nécessaires en cas de litige. Ces données sont conservées au moins sept (7) ans après l'expiration du Certificat, et au maximum dix-sept (17) ans en raison du système de log/archivage de l'AC.
- L'AE pour une durée adéquate, en fonction des exigences légales et réglementaires, et notamment afin d'assurer la continuité du Service et d'apporter les éléments de preuve nécessaires en cas de litige. Ces données sont conservées dix (10) ans ;
- Le Client (uniquement l'ensemble des données collectées en fonction de ses besoins métiers). Le Client définit sa propre période maximale de conservation des données personnelles, en fonction des exigences légales applicables aux Documents gérés par le Client.

De même, aucune copie des données à caractère personnelles ne seront délivrés par l'AE et l'AC sachant que l'Utilisateur possède déjà ses données et qu'il a un exemplaire du Certificat et du Document et de la pièce d'identité utilisée. En conséquence de quoi, le droit à la portabilité ne peut être exercé et aussi car ces données sont des preuves pour l'AE et l'AC.

L'Utilisateur est informé du fait qu'il a le droit de déposer une plainte auprès de la CNIL (https://www.cnil.fr/professionnel).

13 PROPRIÉTÉ INTELLECTUELLE

L'Utilisateur accepte que l'AE et l'AC conservent tous les droits de propriété intellectuelle (brevets, marques déposées et autres droits) relatifs aux éléments constitutifs du Service comme les documents, concepts, technologies, découvertes, procédures, logiciels ou travaux associés aux certificats ainsi qu'aux services connexes devant être fournis par l'AC et l'AE, indépendamment de la forme, langage de programmation, langue ou programme utilisé. Les présentes CGU n'entraînent aucun transfert de droits de propriété intellectuelle relatifs aux Services.

14 ASSURANCE

L'AC et l'AE déclarent avoir souscrit une assurance responsabilité professionnelle relative aux services

entionnés ici, couvrant adéquatement ses obligations conformément aux présentes CGU.

15 SYSTEME JURIDIQUE APPLICABLE, PROCEDURES DE RECLAMATION ET RESOLUTION DES DIFFERENDS

L'AE est responsable du règlement des différends survenant avec l'AE en ce qui concerne le Service et l'AC du règlement des différets survenant avec l'AC.

Les réclamations sont adressées à l'AE ou à l'AC comme indiqué au § 12.

Tout différend se rapportant à la validité, l'interprétation et l'exécution de tout ou partie des présentes CGU relèvera de la compétence des tribunaux français.

Chacune des parties consent de manière irrévocable à la compétence exclusive des juridictions françaises pour régler tout différend ou réclamation découlant du, ou se rapportant, au Service fourni par l'AE et l'AC ou à son objet ou sa formation (y compris, notamment, tout différend ou réclamation de nature non contractuelle).