CONDITIONS GÉNÉRALES D'UTILISATION DU SERVICE DE SIGNATURE ÉLECTRONIQUE AVANCÉE

1 PREAMBULE

L'objet des présentes Conditions Générales d'Utilisation est de définir les conditions juridiques applicables au service permettant de recueillir et d'enregistrer le consentement du Signataire à un Document Électronique émis par l'établissement financier en utilisant une Signature Électronique Avancée reposant sur un Certificat électronique (ci-après le "Service").

Dans le cadre du Service,

DocuSign France est l'Autorité de Certification (AC) en charge :

- D'émettre le Certificat du Signataire,
- De sceller électroniquement le Document Électronique présenté au Signataire au moyen de la clé privée associée au Certificat du Signataire dans un dispositif de création de signature sécurisé.

L'établissement financier est l'Autorité d'Enregistrement (AE) en charge :

- D'authentifier les Signataires,
- De présenter le Document Électronique,
- De recueillir le consentement du Signataire à l'émission du Certificat et à la signature électronique du Document Électronique.

Quicksign est le Prestataire Technique de l'Autorité d'Enregistrement (PTAE) en charge :

- De coordonner avec l'AC le cycle de vie des Certificats et les connexions techniques,
- De réaliser une partie des vérifications d'identité sous-traitées par l'AE,
- De générer un Fichier de Preuve associé à la signature du Document Électronique,
- De transmettre le Fichier de Preuve au tiers archiveur si applicable.

2 DÉFINITION

Autorité de Certification (AC) : désigne DocuSign France, l'entité qui émet les Certificats, en gère le cycle de vie à la demande de l'Autorité d'Enregistrement conformément aux règles et pratiques définies dans la Politique de Certification et procède à la signature du hash du Document Électronique à signer avec la Clé privée associée au Certificat émis. La Politique de Certification applicable peut être consultée sur le site internet de l'AC : https://www.docusign.fr/societe/politiques-de-certifications (Politique de Certification (PC) « PROTECT & SIGN »)

Autorité d'Enregistrement (AE) : désigne l'entité en charge de vérifier et d'authentifier l'identité du Signataire, de collecter les informations utilisées dans le cadre du Protocole de Consentement pour assurer que le consentement est sous le contrôle exclusif du Signataire (telles que le numéro de téléphone portable du Signataire pour lui envoyer l'OTP Code) et de soumettre la demande de Certificats pour permettre au Signataire de signer le Document Électronique. L'AE est en charge de définir les règles de vérification et d'authentification de l'identité des Signataires. L'AE a la possibilité de déléguer tout ou partie de l'implémentation technique de ses règles de vérification d'identité à un ou plusieurs PTAE. Dans le cadre des présentes, l'AE est l'établissement financier.

Certificat : désigne un fichier électronique qui lie les données de validation de la signature électronique à l'identité d'un Signataire donné.

Clé privée : désigne une clé mathématique secrète et unique, contenue dans un dispositif de création de signature, hébergé et géré par l'AC et qui est activée à distance par le Signataire pour signer le Document Électronique.

Document Électronique : désigne le(s) document(s) créé(s) par l'AE devant être signé(s) par le Signataire.

Fichier de preuve : désigne un fichier généré, signé et horodaté par le PTAE qui contient les informations liées à l'authentification du Signataire transmises par l'AE et la transcription du consentement du Signataire à la signature du Document Électronique (y inclus les journaux d'événements techniques liés au consentement). Un Fichier de Preuve dédié est associé à chaque Document Électronique signé afin de prouver la validité de la signature électronique en cas de procédures judiciaires.

Protocole de Consentement : désigne la procédure dans le cadre de laquelle l'AE recueille le consentement du Signataire à :

- L'émission d'un Certificat sous son identité,
- L'acceptation de signer les Documents Électroniques.

OTP code : désigne un mot de passe à usage unique envoyé au Signataire sur son téléphone portable permettant de déclencher l'apposition de la signature électronique.

Politique d'Enregistrement : désigne l'ensemble des règles définies par l'AE pour vérifier et authentifier l'identité du Signataire et recueillir les informations d'enregistrement utilisées pour émettre le Certificat.

Prestataire Technique de l'Autorité d'Enregistrement (PTAE) : désigne le prestataire en charge de récupérer les informations de contacts et d'identité du Signataire, si applicable d'effectuer une partie des mesures techniques de vérification d'identité du Signataire sous-traitées par l'AE, d'envoyer la demande d'émission du Certificat et les documents à signer à l'AC, de créer le Fichier de Preuve, de le sceller, l'horodater et de le mettre à disposition de l'AE. Dans le cadre des présentes, le PTAE est QuickSign.

Signataire : désigne tout individu signant un Document Électronique à l'aide du Service

Signature Électronique Avancée : désigne une signature électronique avancée telle que définie à l'article 3-11 du règlement européen 910/2014 ("eIDAS")

3 OBJET DU SERVICE

Le Service permet :

- De recueillir et d'enregistrer le consentement du Signataire à un Document Électronique en utilisant une Signature Électronique Avancée associée à un Certificat.

- De créer un Fichier de Preuve pour journaliser les événements relatifs à l'acte de Signature Électronique Avancée .

Le Document Électronique signé avec une Signature Électronique Avancée par le biais du Protocole de Consentement est juridiquement contraignant. En effet, il est rappelé dans eIDAS que la Signature Électronique Avancée réalisée par le biais du Service ne peut être refusée au seul motif que cette dernière se présente sous une forme électronique.

4 DESCRIPTION DU SERVICE

Le Signataire est informé et accepte expressément que :

- l'AE identifie le Signataire en conformité avec les règles qu'elle a définies ou auxquelles elle est soumise dans le cadre des contraintes réglementaires liées à la lutte contre le blanchiment et le financement du terrorisme (AML).

- L'AE recueille les informations d'identité et les coordonnées du Signataire (prénom, nom de famille, numéro de téléphone portable, adresse email, date de naissance et toute preuve d'identité).

- L'AE crée un Document Électronique devant être signé par le Signataire.

- Le PTAE transmet à l'AC les informations d'identité et le Document Électronique pour réaliser les opérations de Signature Électronique Avancée.

- L'AC émet le Certificat et procède à la signature du Document Électronique à signer avec la Clé privée associée au Certificat.

Dans cette mesure, le Signataire est informé et accepte expressément que :

- Un Certificat et une clé privée lui soient attribués par l'AC dans le respect de sa PC applicable.

- Le Signataire doit manifester son consentement par le biais de cases à cocher et la saisie de l'OTP code conformément au Protocole de Consentement

- Le PTAE génère un Fichier de Preuve contenant la journalisation des événements associé à la signature du Document Électronique. La conservation du Fichier de Preuve est à la charge de l'AE.

5 OBLIGATIONS DU SIGNATAIRE

En acceptant d'utiliser le Service, le Signataire accepte de respecter les Conditions Générales d'Utilisation et de :

- Fournir des informations d'identité exactes et authentiques ;

- Protéger la sécurité et la confidentialité des informations utilisées pour activer le Protocole de Consentement (tel que l'OTP Code reçu) et s'il s'agit d'un code provisoire (tel qu'un OTP Code) détruire ce dernier après le processus de signature ;

- Vérifier les informations d'identité contenues du Certificat et alerter l'AE si le Certificat n'a pas été rempli correctement.

- Informer rapidement l'AE de tout changement dans les informations d'identité devant figurer dans le Certificat ou dans le Document Électronique.

- Utiliser le Service uniquement pour signer les Documents Électroniques créés par l'AE.

L'AE, le PTAE et l'AC ne sont pas responsables en cas de conséquences dommageables découlant d'un manquement du Signataire à l'obligation de fournir des informations exactes et véridiques.

6 PUBLICATION DU CERTIFICAT

Le Certificat n'est publié ni par l'AC ni par l'AE. Le Certificat est contenu dans le Document Électronique signé et dans le Fichier de Preuve associé au Document Électronique.

7 GESTION DES PREUVES

Le Signataire accepte que les éléments utilisés pour les besoins du Service, en particulier les informations utilisées lors de l'exécution du Protocole de Consentement, le Certificat , les pièces justificatives (par exemple la copie du document d'identité utilisé pour identifier le Signataire etc…) puissent être utilisés comme preuve dans le cadre de procédures judiciaires.

8 DATE PRISE D'EFFET ET DUREE

Les présentes Conditions Générales d'Utilisation prendront effet à la date à laquelle elles seront présentées au Signataire, cette date coïncidant avec la date de demande d'émission du Certificat.

9 SYSTÈME JURIDIQUE APPLICABLE, PROCEDURES ET RÉCLAMATION ET RESOLUTION DES DIFFERENDS

Les Conditions Générales d'Utilisation leur validité interprétation et exécution sont régie par la loi française

Tout différend se rapportant à la validité, l'interprétation et l'exécution de tout ou partie des présentes Conditions Générales d'Utilisation relève de la compétence des juridictions de Paris.