



**Conditions Générales d'Utilisation de la Page
de Consentement de la
Solution de Signature Electronique Goodflag
et des Certificats délivrés par l'AC
Sunnystamp Natural Persons CA**

Version 3.1

Tous droits réservés

Table des matières

1. Introduction	3
2. Définitions et acronymes	3
3. Description du Service	6
3.1 Objet du Service.....	6
3.2 Accès au Service	6
3.3 Services accessoires	6
4. Déroulement d'une Transaction	6
5. Conservation des données	9
6. Obligations du Signataire	10
7. Responsabilité de GOODFLAG	10
8. Sécurité	11
9. Protection des données à caractère personnel	11
10. Confidentialité	13
11. Propriété intellectuelle	13
12. Effets juridiques et convention de preuve	13
13. Nullité partielle	15
14. Loi applicable et attribution de juridiction.....	15
15. Contact	15
16. Annexe	15

1. Introduction

La société LEX PERSONA, dont le siège social est situé 9, avenue du Maréchal Leclerc, 10120 St-André-les-Vergers, France, immatriculée au RCS de Troyes sous le numéro RCS 480 622 257 (ci-après GOODFLAG) met à la disposition de ses Clients une Solution de création de Signature électronique de Documents (ci-après désigné le Service).

Les présentes Conditions Générales d'Utilisation (appelées CGU dans la suite du document), ont pour objet de définir les conditions d'utilisation du Service par les Signataires. Le Signataire reconnaît, avant toute utilisation du Service :

- Avoir pris connaissance des présentes CGU et les accepter sans réserve ;
- Demander, le cas échéant, un Certificat de Signature électronique à son nom, qui sera utilisé, lorsque le mode et le niveau de signature l'exigent, pour signer électroniquement les Documents et les présentes CGU ;
- Disposer de la pleine capacité juridique et des habilitations pour s'engager au titre des présentes CGU.

Les présentes CGU s'appliquent et sont opposables à tout Signataire qui les aura expressément et sans réserve acceptées en cochant la case prévue à cet effet, lorsque celle-ci lui est présentée dans la Page de consentement, lors d'une Transaction réalisée par le Service.

Le Signataire accepte sans réserve les CGU en cochant la case prévue à cet effet sur la Page de consentement lors d'une Transaction réalisée au moyen du Service.

Les présentes CGU sont transmises au Signataire par Goodflag par tout moyen constituant un support durable. Par ailleurs les dernières versions des présentes CGU et de son annexe demeurent téléchargeables au format PDF par le signataire sur leurs liens respectifs.

Les présentes CGU peuvent être modifiées à tout moment par GOODFLAG. Chaque nouvelle version des CGU, numérotée, datée et cachetée électroniquement par la société GOODFLAG, entre en vigueur à compter de la date de sa publication. Les CGU applicables sont celles disponibles en ligne au moment de l'utilisation du Service.

2. Définitions et acronymes

Autorité d'Horodatage (AH) : entité légale qui délivre, dans le cadre d'un Service d'Horodatage, des jetons d'horodatage, qu'elle signe électroniquement, et qui contiennent notamment la date (basée sur une horloge exacte liée au temps universel coordonné), l'empreinte des données horodatées et l'identifiant de la Politique d'Horodatage appliquée. Dans le cas où l'AH est GOODFLAG, la Politique d'Horodatage est disponible sur le site internet de GOODFLAG.

Autorité de Certification (AC) : entité légale chargée de la création, la délivrance, la gestion et la révocation des Certificats au titre de sa Politique de Certification.

Bi-clé : combinaison d'une Clé Privée et d'une Clé Publique utilisée pour effectuer des opérations cryptographiques.

Cachet électronique : données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières. Un Cachet électronique peut être un Cachet électronique simple, avancé ou qualifié au sens du Règlement (UE) no 910/2014 du Parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance.

Certificat : ensemble d'informations garantissant l'association entre l'identité d'une personne physique ou morale et une Clé Publique, grâce à une Signature électronique de ces données effectuée à l'aide de la Clé Privée de l'Autorité de Certification qui délivre le Certificat. Un Certificat contient des informations telles que : la Clé Publique et l'identité de son propriétaire, ses usages autorisés, la durée de vie du Certificat, la Signature électronique du Certificat par l'Autorité de Certification et son identité, etc. Le format standard de Certificat est défini dans la recommandation X.509 v3 et dans la RFC 5280. Dans le cadre des présentes CGU, un Certificat désignera plus particulièrement le Certificat utilisé par le Signataire pour signer. Il pourra s'agir d'un Certificat dont dispose déjà le Signataire ou bien d'un Certificat délivré « à la volée » par l'AC « Sunnystamp Natural Persons CA » gérée par GOODFLAG et généré pour une Transaction de signature particulière.

Clé Privée : clé d'une Bi-clé d'une entité devant être utilisée exclusivement par cette entité.

Clé Publique : clé d'une Bi-clé d'une entité pouvant être rendue publique.

Client : entité légale ayant passée un accord commercial avec GOODFLAG pour utiliser le Service afin de faire signer et/ou Valider électroniquement des Documents à des Signataires et/ou Validateurs par l'intermédiaire de ses Utilisateurs.

Déclaration des Pratiques de Certification (DPC) : ensemble de pratiques qu'une Autorité de Certification met en œuvre pour émettre, gérer, révoquer et renouveler les Certificats qu'elle émet dans le cadre d'une Politique de Certification.

Déclaration d'IGC : document destiné en particulier aux porteurs de Certificats, qui présente et résume les points principaux décrits par la Politique de Certification de l'AC.

Document : tout document sous forme électronique constitutif d'un Parapheur.

Données personnelles : toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Dossier de preuve : ensemble des éléments collectés par le Service pour chaque Transaction permettant ainsi d'assurer la traçabilité et la preuve de la réalisation de la Signature électronique en ligne, et qui peut, le cas échéant, être utilisé en justice aux fins de preuve en cas de litige sur une Signature électronique.

Fournisseur d'identité : entité chargée d'identifier et d'authentifier les Signataires. Le Fournisseur d'identité, après avoir vérifié l'identité du Signataire, produit un Jeton d'identité attestant de cette identité qui est ensuite vérifié par GOODFLAG.

Groupe : ensemble d'Utilisateurs bénéficiant de droits et d'autorisations définis spécifiquement pour ce Groupe. Chaque Utilisateur appartient à un seul Groupe.

Horodatage d'une signature électronique : appelé Horodatage dans le Document, il permet d'attester de la date de Signature électronique d'un Document par le Service d'Horodatage associé au Service, au moyen d'un jeton d'horodatage délivré par une AH aussitôt la Signature électronique effectuée.

Jeton d'identité : donnée électronique produite par un Fournisseur d'identité et attestant de l'identité d'un Signataire.

Liste de Certificats Révoqués (LCR) : fichier daté et signé, comportant, pour une période donnée, les informations relatives aux certificats délivrés par une AC et qui ont été révoqués.

One Time Password (OTP) : code à usage unique généré par le Service et transmis au Signataire par courriel et/ou SMS afin de l'authentifier dans le cas d'une Signature en mode serveur (avec un Certificat à la volée ou avec un Certificat de cachet serveur GOODFLAG).

Page de consentement : ensemble d'écrans HTML exposés par le Service et permettant au Signataire de visualiser et/ou de télécharger les Documents présentés, d'approuver les CGU du Service et d'exprimer explicitement son consentement quant aux Documents soumis à sa Signature électronique.

Parapheur : circuit de Signature(s) et/ou de Validation(s) d'un ou plusieurs Document(s) dont au moins un est soumis à Signature.

Partie(s) : personne(s) physique(s) qui participe(nt) au processus de Signature. Au singulier, il désigne indépendamment l'Utilisateur, le(s) Signataire(s) et/ou le(s) Valideur(s), au pluriel, il désigne l'ensemble.

Politique de Certification (PC) : ensemble de règles auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un Certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes.

Politique d'Horodatage (PH) : ensemble de règles définissant les objectifs et les engagements d'une AH pris pour assurer la fiabilité des services d'horodatage fournis. La PH est un document public accessible librement.

Porteur : désigne la personne, physique ou morale, identifiée dans le Certificat et ayant sous son contrôle la Clé Privée correspondant à la Clé Publique associée au Certificat.

Prestataire de Services de Certification Electronique (PSCE) : entité légale qui délivre des Certificats électroniques et fournit éventuellement d'autres services en matière de certification électronique.

Réponse OCSP : information retournée par l'AC, en temps réel et sur demande, indiquant le statut de révocation d'un Certificat délivré par l'AC.

Service : ensemble des solutions logicielles que GOODFLAG s'engage à fournir aux Signataires pour leur permettre respectivement de signer électroniquement des Documents.

Service d'Horodatage : service fourni par un tiers qui produit, à la demande, un Horodatage d'une signature électronique qui lui est fournie par le Service.

Signataire : personne physique, rattachée ou non à une entité légale, destinataire d'une étape de Signature électronique.

Signature électronique : opération désignant la signature d'un document numérique par un Signataire. Une Signature électronique peut être une Signature électronique simple, avancée ou qualifiée au sens du Règlement (UE) n° 910/2014 du Parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance.

Transaction : ensemble d'opérations successives initiée par un Utilisateur ayant pour finalité la Signature d'un ou plusieurs Document(s) par un Signataire.

Utilisateur : personne habilitée par le Client à se connecter au Service, qui appartient à un Groupe et a des droits particuliers (Gestionnaire de Parapheurs, Signataire, Valideur, etc.).

Valideur : personne physique, représentant ou non une personne morale, destinataire d'une étape de Validation d'un Parapheur.

Validation électronique : opération consistant pour un Valideur à valider électroniquement le(s) Document(s) d'une Transaction, suite à une demande de validation effectuée par l'Utilisateur. L'Utilisateur doit s'assurer, en ce qui concerne l'utilisation de la fonctionnalité de "Demande de validation" (par opposition à une "Demande de signature"), que celle-ci est bien conforme à la définition donnée par le Client en fonction du contexte de la Transaction, et qu'elle est également bien définie par le Client en termes d'exigences vis-à-vis du Valideur.

3. Description du Service

3.1 Objet du Service

Le Service soumis aux présentes CGU a pour objet de permettre la Signature électronique de Document(s) préparé(s) par l'Utilisateur et présenté(s) au Signataire via la Page de consentement et permettre dans le cas d'une signature à la volée avec certificat Goodflag, la délivrance de certificats électroniques. Pour la délivrance de certificats, le service s'appuie sur l'AC Lex Persona CA » de Goodflag délivrant les Certificats aux Signataires devant signer au sein d'une Transaction (la Déclaration d'IGC de cette AC est fournie en Annexe) .

3.2 Accès au Service

Le Service est accessible en ligne, 24h/24, 7j/7, sauf en cas de force majeure, panne, opération de maintenance, de mise à jour ou de problème lié aux réseaux de télécommunication.

Le Service est délivré au Signataire, au moyen de la Page de consentement qui lui est proposée, soit directement, soit via un lien sécurisé contenu dans un courriel d'invitation à signer, pour lui permettre de signer le(s) Document(s) de la Transaction.

3.3 Services accessoires

Le Service s'appuie lui-même sur les services tiers suivants :

- Un ou plusieurs Fournisseur(s) d'identité (tel que la Poste), qui selon le contexte et le choix de l'Utilisateur et du Signataire, peuvent être fourni(s), hébergé(s), exploité(s) par une entité tierce, ou agrégé(s) par un fédérateur d'identité (tel que FranceConnect, France Connect+) ;
- Un [Service d'Horodatage qualifié](#) de GOODFLAG ;
- Un [Service de cachet qualifié](#) de GOODFLAG ;
- Un service d'envoi de courriel ([Brevo](#) – fournisseur français) pour communiquer avec les Utilisateurs et Signataires ;
- Un service d'envoi de SMS ([Smsmode](#) et [Brevo](#) – fournisseurs français) pour communiquer les codes d'authentification aux Signataires le cas échéant.

4. Déroulement d'une Transaction

Les paragraphes ci-dessous décrivent les différentes étapes d'une Transaction.

4.1. Réception d'un courriel contenant une invitation à signer (étape optionnelle). Préalablement à l'utilisation du Service, le Signataire reçoit une invitation à signer, strictement personnelle, à son adresse courriel telle qu'elle

a été définie par l'Utilisateur. De manière alternative, le Signataire peut être invité à signer directement depuis une application Web utilisée par le Client.

4.2. Présentation du contexte de la Transaction. La Transaction démarre et le Signataire est tout d'abord informé du contexte de la Transaction : de qui elle émane, le nom et la description du Parapheur concerné, les nom, prénom et adresse de courriel du Signataire, et, de manière optionnelle, les autres parties prenantes à la Transaction. Le Signataire peut, à ce stade, décider de refuser de signer le Parapheur concerné, ou bien cliquer sur le bouton « Suivant », afin de passer à la Page de consentement. Le cas échéant, d'autres Parapheurs devant être signés par le Signataire, sous réserve qu'ils s'appuient sur le même type de Page de consentement, peuvent être présentés au Signataire afin d'être traités de manière consolidée au sein d'une même Transaction ; dans ce cas, le Signataire peut sélectionner le(s) Parapheur(s) qu'il souhaite intégrer à la Transaction ; il peut également refuser de signer individuellement certains des Parapheurs proposés.

4.3. Présentation de la Page de consentement. La Page de consentement s'affiche dans le navigateur Internet du Signataire. Avant d'apposer sa signature électronique, le Signataire peut remplir les champs dynamiques prévus par la plateforme et configurés par l'Utilisateur. Les champs dynamiques remplis par le Signataire sont inclus dans le document final, figés au moment de l'apposition de la signature. La plateforme garantit que le document signé intègre en amont de la signature le contenu saisi par le Signataire. La Page de consentement présente au Signataire le/les Document(s) à signer et, le cas échéant, les documents à visualiser de manière obligatoire, et le cas échéant, la liste des documents joints qui peuvent être consultés mais qui ne feront pas l'objet d'une Signature électronique. En fonction du paramétrage des Signatures électroniques du ou des Parapheur(s), la Page de consentement peut demander au Signataire de dessiner sa griffe de signature ou de téléverser l'image de cette griffe qui pourra être intégrée dans le(s) Document(s) signé(s) au format PDF.

4.4. Recueil du consentement. Le Signataire coche la case par laquelle il atteste avoir lu et approuvé les présentes CGU, et par ce consentement exprès, il reconnaît la validité et l'opposabilité de la Signature électronique du ou des Document(s).

4.5. Authentification du Signataire. En fonction du paramétrage du Service, la Page de consentement peut ensuite, le cas échéant, demander au Signataire :

- De saisir le code OTP reçu par courriel à l'adresse définie par l'Utilisateur afin d'en vérifier la validité ;
- De saisir le code OTP reçu par SMS sur le numéro de téléphone défini par l'Utilisateur afin d'en vérifier la validité ;
- De téléverser le fichier contenant le scan de sa pièce d'identité afin que la Page de consentement puisse vérifier que les informations de sa pièce d'identité sont conformes aux nom, prénom et pays de nationalité du Signataire tels que définis par l'Utilisateur ;
- De s'authentifier avec FranceConnect, grâce à l'un de ses Fournisseurs d'identité proposés, afin que la Page de consentement puisse vérifier que les informations de son identité sont conformes aux nom, prénom et pays de naissance du Signataire tels que définis par l'Utilisateur ;
- De s'authentifier à l'aide d'un Certificat logiciel ou sur support cryptographique dont le Signataire dispose sur son poste de travail, afin que la Page de consentement puisse vérifier que les informations du Certificat sont conformes aux nom, prénom et pays du Signataire tels que définis par l'Utilisateur ;
- De s'authentifier à l'aide d'un moyen d'identification tel qu'un annuaire d'entreprise ou un réseau social ;

- De s'authentifier avec un moyen d'identification électronique notifié conforme aux exigences énoncées à l'article 8 du règlement eIDAS version 2 en ce qui concerne le niveau de garantie « élevé »¹, afin que la Page de consentement puisse vérifier que les informations d'identité sont conformes aux nom, prénom et pays de naissance du Signataire tels que définis par l'Utilisateur ;
- De s'authentifier avec une méthode d'identification qui permet l'identification d'une personne physique avec un degré de confiance élevé et dont la conformité est confirmée par un organisme d'évaluation de la conformité², afin que la Page de consentement puisse vérifier que les informations d'identité sont conformes aux nom, prénom et pays de naissance du Signataire tels que définis par l'Utilisateur.

Cette liste de moyens d'authentification n'est pas exhaustive. On rappelle que l'objectif de l'authentification est de vérifier, autant que faire se peut, que le Signataire est bien la personne qu'elle prétend être, telle que définie par l'Utilisateur. En cas de Transaction portant sur plusieurs Parapheurs, l'authentification n'est effectuée qu'une seule fois pour l'ensemble des Signatures électroniques effectuées.

4.6. Génération ou utilisation d'un Certificat et création de la Signature. En fonction de la Page de consentement retenue par l'Utilisateur pour le paramétrage du ou des Parapheur(s) concernés par la Transaction, le Signataire peut être amené à signer selon 3 manières différentes.

4.6.1. En mode local avec un Certificat dont dispose le Signataire au préalable

En mode local, la Signature électronique peut être effectuée à l'aide d'un Certificat au format logiciel ou sur support cryptographique au nom du Signataire qui lui est personnel et dont il dispose au préalable. Dans ce cas, le niveau de la Signature électronique au sens du Règlement eIDAS est fonction du type de Certificat utilisé.

La Page de consentement invite le Signataire à ouvrir l'application de création de Signature électronique sur son terminal. Si cette application n'est pas déjà installée sur son poste, le Signataire a la possibilité de la télécharger pour l'installer (ou doit se rapprocher de l'administrateur ayant les droits de procéder à cette installation).

Le Signataire sélectionne ensuite, dans l'application de création de Signature électronique, le Certificat avec lequel il souhaite signer, saisit son code PIN ou son mot de passe si l'application lui demande, et clique sur le bouton « Signer ».

En mode local la Signature électronique est effectuée dans le même temps que l'authentification du Signataire.

Enfin, on notera que la Signature électronique comporte des informations de traçabilité permettant de la relier, via le Dossier de preuve, à la Transaction considérée.

4.6.2. En mode serveur avec un Certificat délivré au nom du Signataire

En mode serveur, la Signature électronique peut être effectuée à l'aide d'un Certificat délivré par l'AC « Sunnystamp Natural Persons CA » au nom du Signataire et généré par la Transaction. Dans ce cas, la Signature électronique peut être de niveau avancé ou qualifié au sens du Règlement eIDAS.

Le Certificat de Signature électronique généré dispose d'une période de validité d'1 (une) heure et ne peut être utilisé que par la Transaction considérée. Les données d'identification qui figurent sur le Certificat sont celles fournies par l'Utilisateur, et qui ont été validées, ou non, lors du processus d'authentification décrit ci-dessus.

¹ Autrement dit, le Certificat qualifié est émis conformément à l'article 24, paragraphe 1, alinéa a, du règlement eIDAS version 2. A date, les moyens d'identification au moins de niveau substantiel ou reconnus localement par l'Etat Membre équivalents à un moyen d'identification de niveau au moins substantiel sont acceptés.

² Autrement dit, le Certificat qualifié est émis conformément à l'article 24, paragraphe 1, alinéa c, du règlement eIDAS version 2.

Ainsi, le niveau qualifié ou avancé de la Signature électronique est respectivement fonction du niveau qualifié ou non qualifié du Certificat et donc du moyen d'authentification du Signataire mis en œuvre.

Enfin, on notera que la Signature électronique comporte des informations de traçabilité permettant de la relier, via le Dossier de preuve, à la Transaction considérée.

4.6.3. En mode serveur sans Certificat

En mode serveur, il est également possible de procéder à une Signature électronique simple au sens du Règlement eIDAS. Dans ce cas, le(s) Document(s) de la Transaction font l'objet d'un Cachet électronique qualifié au sens du règlement eIDAS, destiné à garantir l'intégrité et l'authenticité du ou des Document(s) de la Transaction.

Le Cachet électronique du ou des Document(s) de la Transaction est effectué à l'aide d'un Certificat qualifié au sens du règlement eIDAS de cachet serveur au nom de GOODFLAG.

Enfin, on notera que dans le cas d'une Signature électronique simple, le Cachet électronique, effectué sur chaque Document concerné, comporte des informations de traçabilité permettant de relier ce Cachet électronique, via le Dossier de preuve, à la Transaction considérée.

4.7. Signature du ou des document(s) de la Transaction. Le Signataire clique sur le bouton « Signer ». On rappelle que la ou les Signature(s) électronique(s) considérée(s) ne concernent que le(s) Document(s) à signer de la Transaction et non les pièces jointes optionnelles.

4.8. Fin de la Transaction. Selon les options définies par l'Utilisateur, les personnes concernées, telles que le Signataire et l'Utilisateur, peuvent être notifiées du résultat de la Transaction et disposer d'un lien de téléchargement des Documents signés mis à leur disposition, notamment par voie de courrier électronique.

4.9. Annuler une Transaction. À tout moment, le Signataire peut annuler la Transaction. En revanche ce n'est qu'à l'étape de présentation du contexte de la Transaction que le Signataire peut, de manière explicite, refuser de signer un ou plusieurs Parapheur(s), le cas échéant, en indiquant la raison de ce refus.

5. Conservation des données

Le Service conserve :

- Les Documents constitutifs des Parapheurs ;
- Les données de traçabilité des Transactions de Signature qui sont regroupées dans les Dossiers de preuve générés par le Service, et qui incluent notamment les informations d'identité des Signataires.

Les Dossiers de preuve générés lors de chaque Transaction font l'objet d'un Cachet électronique qualifié au sens du règlement eIDAS par GOODFLAG et sont conservés par le Service de manière à assurer leur intégrité et leur confidentialité. Leur téléchargement par le Client et, le cas échéant, par l'Utilisateur, est possible sous réserve de disposer de l'habilitation nécessaire.

Il incombe au Client de déterminer la durée de conservation nécessaire des Documents et des Dossiers de preuve en application de la législation, des réglementations, ou des procédures des autorités administratives ou juridiques applicables. Sauf conditions particulières, le Service conserve pendant 10 ans les Dossiers de preuves relatifs aux Transactions.

6. Obligations du Signataire

Le Signataire s'engage à :

- Ne signer le(s) Document(s) à travers la Page de consentement qu'en ayant pleinement conscience que sa Signature électronique présentera des effets juridiques potentiellement similaires à ceux qu'aurait sa signature manuscrite sur un document au format papier ;
- N'utiliser aucun dispositif, logiciel ni aucun programme informatique entravant ou risquant d'entraver le fonctionnement du Service, y compris le fonctionnement des communications électroniques, et toutes autres opérations sur le Service ;
- Ne pas porter atteinte au fonctionnement du Service ;
- Être garant de l'exactitude et de toutes les informations communiquées au Service ;
- Assurer la confidentialité du(des) code(s) confidentiel(s) qui lui est(ont) adressé(s).
- Être le seul responsable de la conformité de l'utilisation qu'il fait du Service vis-à-vis des lois et réglementations en vigueur ;
- Le cas échéant, être responsable de la véracité et de l'exactitude des informations qu'il saisit dans les champs dynamiques ;
- Informer le Client et/ou l'Utilisateur de toute défaillance ou dysfonctionnement constaté du Service.

7. Responsabilité de GOODFLAG

7.1. Généralités

GOODFLAG met à disposition des Signataires une prestation techniques permettant la création de signatures électroniques. Lorsque GOODFLAG agit en qualité de prestataire de service de confiance pour la création de signature électronique et de certificats non qualifiés et en tant que prestataire de services de confiance qualifié (QTSP) pour la délivrance de certificats, cachets qualifiés ou horodatage qualifié., elle assume l'ensemble des obligations légales prévues par le règlement (UE) n° 910/2014 dit « eIDAS » (et ses textes modificatifs, notamment eIDAS 2).

Dans ce cadre, GOODFLAG est tenue aux responsabilités légales prévues par le règlement eIDAS et par le droit français, notamment :

- Responsabilité en cas de manquement intentionnel ou par négligence aux obligations légales du prestataire de services de confiance, avec renversement de la charge de la preuve conformément à l'article 13 du règlement eIDAS ;
- Responsabilité du fait des produits défectueux au sens de la directive 85/374/CEE et des articles 1245 et suivants du Code civil, laquelle ne peut être exclue ni limitée.

La responsabilité de GOODFLAG couvre aussi la sécurité, l'intégrité et la traçabilité technique du processus de signature, y compris les champs dynamiques décrits dans le déroulé de la transaction.

Pour les services qui ne relèvent pas d'un service de confiance eIDAS, GOODFLAG n'assume qu'une obligation de moyens et ne pourra être tenue pour responsable des dommages résultant :

- D'une utilisation du Service non conforme à la réglementation applicable aux Documents signés ;

- D'un usage inapproprié ou frauduleux par un Signataire ou un tiers.

Dans tous les cas, cette limitation ne s'applique pas en cas de faute lourde ou de dol de GOODFLAG.

Sauf engagement contractuel spécifique (par exemple accord de niveau de service – SLA), GOODFLAG ne garantit pas un fonctionnement ininterrompu ou exempt d'erreurs du Service et exclut, dans les limites légales, toute garantie implicite de performance ou d'adéquation à un besoin particulier.

8. Sécurité

GOODFLAG s'engage à déployer ses meilleurs efforts, conformément aux règles de l'art, pour sécuriser le Service et assurer la confidentialité, l'intégrité et la disponibilité des données.

Dans le cadre de son accès au Service, il est expressément rappelé au Signataire qu'Internet n'est pas un réseau sécurisé. Dans ces conditions, il appartient au Signataire de prendre toutes les mesures appropriées de façon à protéger ses propres données et logiciels, notamment des détournements éventuels et de la contamination par d'éventuels virus circulant sur le réseau Internet ou de l'intrusion d'un tiers dans son système d'information.

GOODFLAG peut prendre toutes les mesures d'urgence nécessaires à la sécurité du Service.

9. Protection des données à caractère personnel

GOODFLAG met en œuvre des traitements de données personnelles pour le compte du Client afin de fournir le Service et plus particulièrement, de permettre au Signataire d'être identifié et authentifié, d'apposer sa Signature électronique sur le Document et de constituer et conserver le Dossier de preuve.

Au sens du Règlement Européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, GOODFLAG intervient en qualité de sous-traitant et le Client intervient en qualité de responsable de traitement.

De ce fait GOODFLAG est autorisée à collecter, traiter et héberger, pour le compte du Client, les données à caractère personnel des Signataires nécessaires pour fournir le Service.

Les données à caractère personnel d'un Signataire qui peuvent être traitées par GOODFLAG pour la fourniture du Service dépendent du type de Signature électronique exigé par l'Utilisateur (ex : Signature électronique en mode local ou en mode serveur, type de Certificat délivré, etc.) et sont présentées dans le tableau ci-dessous. Il est précisé que le fondement légal et la durée de conservation sont **indiqués à titre indicatif** dans la mesure où ces derniers dépendent des instructions du Client.

Donnée personnelle	Finalité	Fondement légal	Durée de conservation
Nom de famille	Identification du Signataire et enregistrement dans le Dossier de preuve	ETSI EN 319 411-1 [LCP] et ETSI EN 319 411-2 [QCP-n-qscd] dans le cas d'un Certificat à la volée Contrat entre le Client et Goodflag	Dépend des instructions du Client (7 ans minimum dans le cas d'un Certificat à la volée)
Prénom(s)	Identification du Signataire et enregistrement dans le Dossier de preuve	ETSI EN 319 411-1 [LCP] et ETSI EN 319 411-2 [QCP-n-qscd] dans le cas d'un Certificat à la volée Contrat entre le Client et Goodflag	Dépend des instructions du Client (7 ans minimum dans le cas d'un Certificat à la volée)
Pays de naissance, nationalité ou pays de délivrance de la pièce d'identité vérifiée	Identification du Signataire et enregistrement dans le Dossier de preuve	ETSI EN 319 411-1 [LCP] et ETSI EN 319 411-2 [QCP-n-qscd] dans le cas d'un Certificat à la volée Contrat entre le Client et Goodflag	Dépend des instructions du Client (7 ans minimum dans le cas d'un Certificat à la volée)
Numéro de portable	Envoi d'un OTP SMS pour la Signature électronique en mode serveur afin d'authentifier le Signataire et enregistrement dans le Dossier de preuve	ETSI EN 319 411-1 [LCP] dans le cas d'un Certificat à la volée Contrat entre le Client et Goodflag	Dépend des instructions du Client (10 ans par défaut)
Adresse IP	Enregistrement dans le Dossier de preuve	Contrat entre le Client et Goodflag Nécessaire au Service	Dépend des instructions du Client (10 ans par défaut)
Autres données personnelles présentes dans le scan de la pièce d'identité	Délivrance d'un Certificat à la volée de niveau ETSI LCP suite à la vérification de la pièce d'identité du Signataire	ETSI EN 319 411-1 [LCP] Contrat entre le Client et Goodflag	Maximum 17 ans ³
Autres données pouvant se trouver dans un Jeton d'identité (comme la date de naissance par exemple)	Enregistrement dans le Dossier de preuve	Contrat entre le Client et Goodflag Nécessaire au Service	Dépend des instructions du Client (10 ans par défaut)
Données personnelles renseignées dans les documents à signer	Stockage sécurisé des documents signés dans le cas où le Client a confié cette mission à GOODFLAG	Contrat entre le Client et Goodflag	Dépend des instructions du Client

GOODFLAG agit pour le compte et sous instruction du Client. Le Client est responsable du traitement effectué sur les données collectées par lui-même ou par GOODFLAG en sa qualité de sous-traitant.

GOODFLAG s'engage à ne pas divulguer à des tiers autres que ses sous-traitants ou des tribunaux (à des fins juridiques), les données à caractère personnel relatives à chaque Signataire sans l'autorisation préalable de la personne concernée. La liste complète des sous-traitants impliqués dans le service est disponible sur à ce [lien](#).

Toute opposition du Signataire à la conservation de ses données personnelles empêche la délivrance d'un Certificat et la création de Signature électronique. Le Signataire peut communiquer au Client toute demande relative à l'accès et/ou à la rectification des données le concernant, ainsi qu'à l'opposition et à la suppression de ses données pour des motifs légitimes.

Pour exercer ces droits ou pour toute question sur le traitement de vos données dans ce dispositif, vous pouvez contacter le DPO de GOODFLAG : dpo@goodflag.com.

Si vous estimez, après nous avoir contactés, que vos droits « Informatique et Libertés » ne sont pas respectés, vous pouvez adresser une réclamation à la CNIL.

10. Confidentialité

GOODFLAG prendra toutes les mesures nécessaires pour protéger les informations confidentielles échangées sur le Service. Il est interdit aux Signataires de dévoiler des informations confidentielles acquises lors de la Transaction sur le Service.

Ces dispositions ne font pas obstacle aux communications ordonnées par voie judiciaire ou administrative.

11. Propriété intellectuelle

Tous les éléments composant le Service, les documentations et toutes autres informations remises par GOODFLAG sont et restent la propriété exclusive de GOODFLAG. Toute utilisation ou reproduction, totale ou partielle, de ces éléments et/ou des informations qu'il contient, par quelque procédé que ce soit, est strictement interdite et constitue une contrefaçon susceptible de poursuites à l'exclusion des utilisations et reproduction préalablement et expressément autorisées.

Les présentes CGU n'emportent aucune cession des droits de propriété intellectuelle dont GOODFLAG est le titulaire.

Toute utilisation ou reproduction, totale ou partielle, par quelque procédé que ce soit est strictement interdite et constitue une contrefaçon susceptible de poursuites à l'exclusion des utilisations et reproduction préalablement et expressément autorisées.

L'Utilisateur et/ou le Client déclare détenir et conserver la libre disposition des droits de propriété intellectuelle des Documents destinés à être utilisés dans le cadre du Service. L'utilisation du Service n'emporte aucune cession de droit de propriété intellectuelle dont l'Utilisateur et/ou le Client est le titulaire.

12. Effets juridiques et convention de preuve

Lorsqu'elle garantit l'identité du signataire et l'intégrité du Document signé, la Signature électronique à la même valeur juridique que la Signature manuscrite. Elle ne peut être contestée au seul motif qu'elle se présente sous forme électronique. En revanche, le niveau de sécurité varie selon le niveau de Signature électronique. Dès lors,

³ Le scan de la pièce d'identité contenant notamment la photographie de son propriétaire n'est pas conservé mais les informations textuelles contenues dans la pièce le sont, d'une part, pour ne pas redemander au Signataire de retransmettre, à chaque fois qu'il doit signer des documents, sa pièce d'identité, tant qu'elle est en cours de validité et d'autre part, pour respecter les exigences de la norme ETSI EN 319 411-1 sur la durée de conservation de ces données.

les Parties s'engagent à ne pas contester la recevabilité, l'opposabilité ou la force probante des éléments du Document signé au moyen du Service, sur le fondement de leur nature électronique.

Tout contrat conclu par des moyens électroniques selon la procédure décrite dans les CGU est formé lorsque le Document porte la Signature électronique de chaque Partie.

Les Parties reconnaissent et conviennent expressément que :

- la transmission électronique du Document signé au moyen d'une Signature électronique à travers le Service vaut preuve, entre les Parties, de l'existence, de l'origine, de l'envoi, de l'intégrité et de l'horodatage du Document ainsi signé par l'une des Parties et de la réception du Document signé par l'autre Partie ; étant précisé que l'envoi et la réception sont réputés intervenir au même instant ;
- le processus de Signature électronique d'un Document signé requiert nécessairement un mode de fonctionnement asynchrone impliquant qu'une des Parties signe avant l'autre Partie. En conséquence, les Parties conviennent expressément que la première signature d'un Document avec une Signature électronique devant être signé par les deux Parties ne constitue pas une offre ou un engagement unilatéral de volonté de la première Partie ayant apposé sa Signature électronique sur le Document ;
- la date de Signature électronique du Document sera la date mentionnée dans ledit Document par le ou les Signataires.

Les Parties reconnaissent aux Documents signés au moyen du Service la qualité de document original et les admettent comme preuve recevable entre elles, au même titre qu'un écrit sur support papier, dans toute hypothèse.

Les Parties acceptent que les éléments d'identification utilisés dans le cadre du Service, notamment les Certificats utilisés, soient admissibles devant les Tribunaux et fassent preuve de l'identité du Signataire.

Le Signataire reconnaît avoir communiqué tous les éléments permettant d'assurer son identification.

Les Signataires, dont la Signature électronique a été utilisée pour signer le Document, sont réputés être dûment habilités à signer par la Partie à laquelle ils appartiennent et à engager juridiquement ladite Partie. A ce titre, il appartient à chaque Partie de veiller à ce que le Signataire dispose des délégations de pouvoirs nécessaires. Le défaut d'une Partie dans la gestion de ces délégations de pouvoirs ne pourra pas être opposé à l'autre Partie pour faire échec à la valeur juridique du Document signé.

Les Parties acceptent que :

- (i) Le Signataire manifeste son consentement selon protocole décrit à l'article 4.3. des présentes CGU ;
- (ii) Les actions visées dans le (i) ci-dessus sont admissibles devant les Tribunaux et font preuve des données et des faits qu'elles matérialisent ainsi que des signatures et des procédés d'authentification qu'elles expriment conformément à la réglementation applicable ;
- (iii) Le contrat signé avec une Signature électronique ne peut conférer plus de droits ou d'obligations aux Parties que s'il avait été établi, signé et conservé sur support papier ;
- (iv) Les présentes CGU ne modifient pas les règles générales et spéciales de validité, d'exécution et de fin des contrats ;

- (v) Les dates certifiées électroniquement sont admissibles devant les Tribunaux et font preuve des données et des éléments qu'elles contiennent. Les Parties reconnaissent que l'établissement de tous les Documents sera effectué conformément à l'heure du Temps Universel Coordonné (UTC) ;
- (vi) Les courriers électroniques émis par le Service concernant le processus de Signature, les Documents signés dans le cadre du Service et les Dossiers de preuve sont admissibles devant les Tribunaux et font preuve des données et des éléments qu'ils contiennent.

Les Parties reconnaissent que le Service répond aux dispositions légales et réglementaires en vigueur en matière de contractualisation par voie électronique.

13. Nullité partielle

Toute disposition des CGU qui viendrait à être déclarée nulle ou illicite par un juge sera privée d'effet. La nullité d'une telle disposition ne saurait porter atteinte aux autres dispositions des CGU ni affecter leur validité dans leur ensemble ou leurs effets juridiques.

14. Loi applicable et attribution de juridiction

Les présentes CGU sont soumises au droit français.

En cas de litige, les parties tenteront de rechercher une solution amiable. En cas d'impossibilité de résoudre le litige à l'amiable au-delà d'un délai de 3 mois à compter de la première notification, la plus diligente des parties soumettra ledit litige à l'appréciation du Tribunal de Troyes.

15. Contact

Pour toute réclamation ou question sur l'utilisation et le fonctionnement du Service, le Signataire peut contacter le support du Client qui lui a soumis le(s) Document(s) à signer.

16. Annexe

La Déclaration d'IGC ci-dessous de l'AC « Sunnystamp Natural Persons CA » de GOODFLAG s'applique uniquement dans le cas d'une Signature en mode serveur avec Certificat à la volée.

Contact de l'AC	Lex Persona (nom commercial « Goodflag » 9 AVENUE MARECHAL LECLERC 10120 ST ANDRE LES VERGERS FRANCE Adresse courriel : pki@sunnystamp.com Téléphone : +33 (0)3 25 43 90 78
Site de publication	Les informations, énumérées dans la section 2.2 de la PC/DPC, sont publiées sur le site de publication de l'AC : https://pki2.sunnystamp.com/repository . Le site de publication est disponible 24h/24 et 7j/7 en conditions normales de fonctionnement.
Types de Certificats émis	L'AC délivre des Certificats à des personnes physiques pouvant être rattachées ou non à une Entité Légale. Ces Certificats ont une durée de validité maximale d'une (1) heure et ne

	<p>peuvent être utilisés que pour signer les documents de la Transaction de signature pour laquelle ils ont été spécialement créés.</p> <p>L'AC délivre cinq types de Certificats :</p> <ol style="list-style-type: none"> 1. Les certificats utilisés par ses répondeurs OCSP pour signer les réponses OCSP ; 2. Les certificats « ETSI LCP avec possibilité de révocation » avec l'OID 1.3.6.1.4.1.22542.100.1.1.1.2, conformes à la norme [EN 319 411-1] pour le niveau LCP ; 3. Les certificats « OPEN REG » avec l'OID 1.3.6.1.4.1.22542.100.1.1.1.3, pour lesquels la présente PC/DPC laisse l'Autorité d'Enregistrement libre de définir le processus d'enregistrement appliqué pour authentifier et vérifier l'identité des Signataires ; 4. Les certificats « FranceConnect » avec l'OID 1.3.6.1.4.1.22542.100.1.1.1.4, délivrés à la suite d'une authentification du Signataire par un Fournisseur d'identité proposé par FranceConnect (https://franceconnect.gouv.fr) ; 5. Les certificats « MIE eIDAS » avec l'OID 1.3.6.1.4.1.22542.100.1.1.1.5, conformes à la norme [EN 319 411-2] pour le niveau QCP-n-qscd, délivrés à la suite d'une authentification du Signataire via un moyen d'identification électronique : <ul style="list-style-type: none"> Ayant fait l'objet d'une notification par l'un des États membres de l'Union européenne ; et Ayant un niveau de garantie substantiel ou élevé ; et Pour lesquels il est publié une documentation en langue anglaise ou française permettant d'établir, sans ambiguïté, que la présence de la personne physique ou un représentant autorisé de la personne morale est un prérequis à l'obtention de ce moyen d'identification électronique ; 6. Les certificats « ETSI LCP sans possibilité de révocation » avec l'OID 1.3.6.1.4.1.22542.100.1.1.1.6, conformes à la norme [EN 319 411-1] pour le niveau LCP. Les Certificats sont émis par l'AC « Sunnystamp Natural Persons CA », qui est elle-même émise par l'AC racine « Sunnystamp Root CA G2 ». <p>Les certificats de ces AC sont disponibles à l'adresse suivante : https://pki2.sunnystamp.com/repository</p> <p>L'AC peut délivrer des certificats de test, lesquels sont identifiés par le préfixe « TEST- » dans les attributs SN et GN du sujet.</p>
Objet des Certificats	Les Certificats émis par l'AC sont des certificats de Signature électronique à destination de personnes physiques, et qui, dans le cas des Certificats OPEN REG et MIE eIDAS, peuvent être rattachées à une entité légale.
Modalités d'obtention	<p>La demande d'un Certificat provient du besoin par le Signataire de signer, au sein d'une Transaction de Signature électronique, les documents que lui a soumis le Client.</p> <p>Validation de l'identité du Signataire :</p> <p><u>Pour les Certificats ETSI LCP sans possibilité de révocation :</u></p> <p>Le Client doit fournir à l'Autorité d'Enregistrement (appelée AE dans la suite du document) les nom, prénom(s) et numéro de téléphone portable du Signataire devant signer les documents.</p>

	<p>Le Signataire doit ensuite saisir l'OTP SMS que lui a envoyé l'AE et transmettre à l'AE un document officiel d'identité (carte nationale d'identité, passeport ou carte de séjour) en cours de validité avec photographie comportant ses nom, prénom(s), date et lieu de naissance.</p> <p><u>Pour les Certificats OPEN REG :</u></p> <p>Le Client doit fournir au minima à l'AE les nom et prénom(s) du Signataire devant signer les documents.</p> <p>Le Client décrit et documente la manière dont il procède pour vérifier l'identité du Signataire et l'authentifier à l'aide des moyens d'authentification proposés.</p> <p><u>Pour les Certificats FranceConnect et MIE eIDAS :</u></p> <p>Le Client doit fournir au minimum à l'AE les nom et prénom(s) du Signataire devant signer les documents.</p> <p>L'AE délègue la validation de l'identité du Signataire à FranceConnect, ou bien respectivement à un organisme qui met en place un moyen d'identification électronique, et récupère auprès de celui-ci les informations d'identité suivantes du Signataire :</p> <ul style="list-style-type: none"> Nom de naissance ; Prénom(s) ; Date de naissance ; Pays de naissance. <p>Utilisation de la Clé Privée et du Certificat par le Signataire pour signer :</p> <p>La Clé Privée d'un Signataire est protégée par le Service qui met en œuvre des moyens techniques et organisationnels pour garantir que seul le propriétaire de cette Clé Privée puisse l'utiliser pour signer.</p> <p>Dans le cas d'un Certificat ETSI LCP avec ou sans possibilité de révocation, FranceConnect ou MIE eIDAS, la clé privée du Signataire est générée et stockée sur un HSM certifié FIPS 140-2 level 3 et QSCD et figurant sur la liste [UE_QSig/SealCD].</p>
Modalités de renouvellement	Il n'y a pas de processus de renouvellement.
Modalités de révocation	La révocation d'un Certificat est déclenchée automatiquement dès lors que le Signataire annule la Transaction de signature pour laquelle le Certificat a été spécialement créé. Cette annulation se produit dans les cas suivants : • Si le Signataire refuse de signer les documents de la Transaction de signature ; • Si le Signataire ne valide pas les informations contenues dans son Certificat qui lui sont présentées dans la page de signature à la suite de la génération de son Certificat.
Limites d'usage	Les Certificats délivrés par l'AC ont une durée de validité maximale de 1 heure et sont utilisés par les Signataires pour signer exclusivement les documents de la Transaction de Signature électronique pour laquelle ils ont été spécialement créés.

	<p>L'AC ne peut être tenue responsable de l'utilisation du Certificat d'une manière non conforme à la PC/DPC.</p> <p>Un Certificat délivré par l'AC peut être utilisé pour valider les Signatures électroniques créées par la personne physique qui est le propriétaire du Certificat.</p> <p>Les informations du dossier d'enregistrement ainsi que les traces des événements liés au cycle de vie des Certificats sont conservées par l'AC pendant une durée maximale de 7 ans.</p>
Obligations des Signataires	<p>Le Signataire à l'obligation de :</p> <ul style="list-style-type: none"> • Respecter les modalités d'usages précisées dans le chapitre 4.5 de la PC/DPC ; • Fournir des informations correctes à l'AE lors de la phase d'enregistrement ; • Confirmer l'exactitude des informations contenues dans son Certificat ; • Informer l'AE de toute modification des informations contenues dans son Certificat.
Obligations des Clients	<p>Le Client à l'obligation de :</p> <ul style="list-style-type: none"> • Respecter les modalités d'usages précisées dans le chapitre 1.4 de la PC/DPC ; • Fournir des informations correctes à l'AE lors de la phase d'enregistrement ; • Informer l'AE de toute modification des informations contenues dans le Certificat.
Obligations de vérification des certificats par les UC	<p>Les UC ont l'obligation de :</p> <ul style="list-style-type: none"> • Vérifier et respecter l'usage pour lequel le Certificat a été émis ; • Utiliser le logiciel et le matériel adéquat pour la vérification de la validité du Certificat. <p>Il est rappelé aux UC que les certificats de test ne sont produits qu'à des fins de test technique ou de démonstration et n'engagent ni l'AC ni la personne qui les utilise.</p>
Limite de responsabilité	<p>Goodflag ne pourra pas être tenue pour responsable d'une utilisation non autorisée ou non conforme des données d'authentification, des certificats, des LCR, ainsi que de tout autre équipement ou logiciel mis à disposition.</p> <p>Goodflag décline sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans les certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées par le Signataire.</p>
Références documentaires	<p>La PC/DPC de l'AC est disponible à l'adresse suivante : https://pki2.sunnystamp.com/repository.</p>
Condition d'indemnisation	<p>Sans objet.</p>
Loi applicable et gestion des litiges	<p>Les présentes CGU sont soumises au droit français.</p> <p>En cas de litige entre les parties découlant de l'interprétation, l'application et/ou l'exécution du contrat et à défaut d'accord amiable entre les parties ci-avant, la compétence exclusive est attribuée au tribunal de commerce de Troyes.</p> <p>L'AC dispose d'une procédure de gestion des plaintes et réclamations qui consiste pour le demandeur à ouvrir un ticket sur le site de support de l'AC : https://support.goodflag.com.</p>

Gestion des données à caractère personnelles	L'AC prend toutes les mesures nécessaires pour que les données personnelles soient protégées et stockées de manière à garantir leur intégrité et leur confidentialité conformément à la loi française N°78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés et modifications à venir ainsi que le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.
Audits et références applicables	<p>L'AC est certifiée conforme :</p> <ul style="list-style-type: none">- Pour les certificats émis selon la politique 1.3.6.1.4.1.22542.100.1.1.1.2, à la norme [EN 319 411-1] pour le niveau LCP ;- Pour les certificats émis selon la politique 1.3.6.1.4.1.22542.100.1.1.1.6, à la norme [EN 319 411-1] pour le niveau LCP ;- Pour les certificats émis selon la politique 1.3.6.1.4.1.22542.100.1.1.1.5, à la norme [EN 319 411-2] pour le niveau QCP-n-qscd et au référentiel d'exigences [ANSSI_QCP]. <p>Le certificat de conformité est valable 2 ans et est délivré à la suite d'un audit réalisé par un organisme accrédité selon la norme [EN 319 403]..</p>