



Conditions Générales d'Utilisation

Goodflag Community

Version 1.8

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 Gratuité du service	6
3.4 Services accessoires.....	6
4. Utilisation du Service par l'Utilisateur.....	7
5. Utilisation du Service par le Signataire.....	7
5.1 Réception d'un courriel contenant une invitation à signer	7
5.2 Présentation du contexte de la Transaction	7
5.3 Présentation de la Page de consentement	8
5.4 Recueil du consentement	8
5.5 Authentification du Signataire	8
5.6 Génération ou utilisation d'un Certificat et création de la Signature.....	9
5.6.1 En mode serveur avec un Certificat délivré au nom du Signataire	9
5.6.2 En mode serveur sans Certificat.....	9
5.7 Signature du ou des document(s) de la Transaction	9
5.8 Fin de la Transaction.....	9
5.9 Annuler une Transaction.....	9
6. Conservation des données	10
7. Obligations de l'Utilisateur et du Signataire.....	10
8. Responsabilité de GOODFLAG	11
9. Droit de rétractation.....	12
10. Sécurité	12
11. Protection des données à caractère personnel	13
11.1 Données à caractère personnel des Signataires	13
11.1.1 Cas général	13
11.1.2 Aspects propres à la Signature électronique avancée.....	14
11.1.3 Aspects propres à la Signature qualifiée.....	15
11.2 Données à caractère personnel de l'Utilisateur	15
12. Confidentialité.....	15
13. Propriété intellectuelle.....	15
14. Effets juridiques et convention de preuve	16
14.1 Effets juridiques d'une Signature électronique.....	16
14.2 Le Dossier de Preuve.....	17
15. Contact	17
16. Mentions Légales	18
17. Hébergement	18
18. Force majeure	18
19. Droit applicable – Langue	18
20. Litiges.....	18
21. Attribution de la conception du Site Internet et coordonnées de l'éditeur.....	19
22. Annexe 1	19
23. Annexe 2	22

1. Introduction

La société LEX PERSONA, dont le siège social est situé 9, avenue du Maréchal Leclerc - 10120 St-André-les-Vergers, immatriculée au Registre du Commerce et des Sociétés de Troyes sous le numéro 480 622 257 (ci-après « **GOODFLAG** ») met à la disposition des Utilisateurs et Signataires une plateforme gratuite appelée « Goodflag Community » (ci-après désignée le « **Service** ») qui permet 1) à un Utilisateur de créer un Compte Utilisateur pour faire signer électroniquement un ou plusieurs Document(s) à un ou plusieurs Signataire(s), et 2) à un Signataire de signer le(s) Document(s) qui lui sont soumis à la signature électronique par le(s) Utilisateur(s).

Les caractéristiques et fonctionnalités principales du Service, sont présentées dans les articles 3 et 4 ci-dessous ainsi que sur le site Internet du Service, accessible [ici](#). L'Utilisateur et le Signataire peuvent également se référer au Cahier des fonctionnalités du Service fourni en annexe 2 des présentes CGU, qui décrit l'ensemble des fonctionnalités offertes par le Service.

L'Utilisateur est tenu d'en prendre connaissance avant toute inscription.

Les présentes Conditions Générales d'Utilisation (les « CGU »), ont pour objet de définir les conditions d'utilisation du Service par les Signataires et Utilisateurs tel que définis ci-dessous.

Le Signataire et l'Utilisateur reconnaissent, avant toute utilisation du Service :

- Avoir pris connaissance des présentes CGU et les accepter sans réserve ;
- Disposer de la pleine capacité juridique et avoir tout pouvoir pour s'engager au titre des présentes CGU.

Le Signataire reconnaît également demander et accepter d'utiliser un Certificat de Signature électronique à son nom qui sera utilisé, dès lors que le mode et le niveau de signature l'exigent, pour signer électroniquement les Documents et les présentes CGU.

Les présentes CGU s'appliquent et sont opposables à tout Signataire et Utilisateur qui les aura expressément et sans réserve acceptées a) 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 concernant le Signataire et/ou b) en cliquant sur le bouton Accepter lors du processus d'inscription du portail utilisateur concernant l'Utilisateur.

Les présentes CGU sont téléchargeables au format PDF par le Signataire depuis la Page de consentement et/ou depuis la page d'acceptation lors du processus d'inscription.

Les présentes CGU peuvent être modifiées à tout moment par GOODFLAG. Chaque nouvelle version des CGU, numérotée 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 [ici](#) au moment de l'utilisation du Service.

Après avoir pris connaissance des présentes CGU et s'il vous reste des questions, n'hésitez pas à les poser au support Goodflag Community à l'adresse support-at-goodflag.community, en veillant à remplacer « -at- » par le symbole « @ ».

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 contexte du Service, l'AH est gérée par GOODFLAG et 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 eIDAS.

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 généralement celui utilisé par le Signataire pour signer et qui lui est délivré « à la volée » par l'AC « Sunnystamp Natural Persons CA » gérée par GOODFLAG et dédié à une Transaction de Signature électronique avancée ou qualifiée. Ce terme peut également désigner celui utilisé par le Service pour effectuer un Cachetage du ou des Document(s) associé(s) à une Transaction de Signature électronique simple.

Certificat de Preuve : rapport détaillé au format PDF listant les principales caractéristiques d'un Parapheur (informations générales, Étapes, Documents, Validateurs, Signataires, etc.), ainsi que les principaux événements de son cycle de vie (création, signatures, archivage, etc.). Le Certificat de Preuve est disponible tout au long du cycle de vie du Parapheur et il est cacheté électroniquement par la plateforme dès que le Parapheur passe en statut « archivé ». Il est alors dans sa version définitive et infalsifiable.

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.

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 : désigne 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 d'un Parapheur permettant ainsi d'assurer la traçabilité et la preuve de la réalisation des signatures en ligne, et qui peut, le cas échéant, être utilisé en justice aux fins de preuve en cas de litige sur une Signature électronique produite par le Service.

Fichier de Preuve : fichier XML cacheté et horodaté par GOODFLAG, intégré dans un Dossier de Preuve, qui rassemble l'ensemble des éléments constitutifs d'une Transaction de signature électronique au sein d'un Parapheur, permettant d'assurer la traçabilité et la preuve de la réalisation des signatures effectuées, et qui peut, le cas échéant, être utilisé en justice aux fins de preuve en cas de litige.

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.

Horodatage d'une signature électronique : donnée permettant 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.

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

Règlement eIDAS : règlement de l'Union européenne n° 910/2014 du Parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance. Lorsque il est fait spécifiquement référence à des modifications apportées par le règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le Règlement eIDAS, on citera alors le Règlement eIDAS (« version 2 »).

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 désignée par l'Utilisateur pour signer le(s) Document(s) d'une Transaction.

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 eIDAS.

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

Utilisateur : personne physique ayant créé un Compte Utilisateur afin d'initier une ou plusieurs Transactions permettant de faire signer électroniquement des Documents à des Signataires.

3. Description du Service

3.1 Objet du Service

Le Service soumis aux présentes CGU a pour objet de permettre la Signature de Document(s) préparé(s) par l'Utilisateur et présenté(s) au Signataire via la Page de consentement.

3.2 Accès au service

Le Service est accessible en ligne, 24h/24, 7j/7, sauf cas de force majeure tel que prévu à l'article 18 ci-dessous pannes, opérations de maintenance, de mise à jour ou de problèmes liés aux réseaux de télécommunication.

Le Service est délivré au Signataire, au moyen de la Page de consentement qui lui est proposée 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 Gratuité du service

Le Service est fourni à l'Utilisateur par GOODFLAG à titre gratuit sous réserve que l'Utilisateur est un particulier, un travailleur indépendant ou un membre d'une association.

Les Données Personnelles des Utilisateurs et des Signataires ne seront pas utilisées à des fins commerciales ou marketing et ne pourront être vendues.

GOODFLAG s'engage à n'utiliser, à des fins de communication, que des données anonymisées portant sur le nombre de Comptes Utilisateurs et sur le nombre de Signatures électroniques générées par le Service.

La seule contrepartie que GOODFLAG pourrait dégager de l'utilisation du Service est la notoriété apportée par la multiplication des Utilisateurs, Signataires, Parapheurs et Signatures.

3.4 Services accessoires

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

- L'AC « Sunnystamp Natural Persons 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 1), en mode serveur avec Certificat à la volée ;
- Un ou plusieurs Fournisseurs d'identité, 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 pour la Signature électronique avancée ou France Identité pour la Signature électronique Qualifiée) ;

- Un Service d'Horodatage de GOODFLAG ;
- Un Service d'envoi de courriels et de SMS (Brevo – fournisseur français), pour communiquer avec les Utilisateurs et Signataires et pour communiquer les codes d'authentification aux Signataires, le cas échéant ;
- Un Service d'envoi de SMS (Smsmode – fournisseur français), pour communiquer les codes d'authentification aux Signataires, le cas échéant.

4. Utilisation du Service par l'Utilisateur

Pour utiliser le Service, l'Utilisateur doit se référer au Cahier des fonctionnalités du Service qui décrit l'ensemble des fonctionnalités offertes par le Service à l'Utilisateur et dont lien est fourni en annexe 2.

Le Compte Utilisateur peut être supprimé à tout moment par l'Utilisateur via la procédure décrite dans le formulaire accessible [ici](#). La suppression du Compte Utilisateur entraîne la suppression des Parapheurs de l'Utilisateur, mais n'entraîne pas la suppression des Contacts liés au Compte Utilisateur qui ne sont accessibles que par ce dernier : il appartient donc à l'Utilisateur d'effectuer manuellement les suppressions nécessaires.

En substance, l'Utilisateur doit compléter le formulaire de demande de suppression d'un compte Utilisateur et signer ce formulaire à l'aide d'un Parapheur créé depuis un compte Goodflag Community dont l'adresse de courriel du Signataire correspond à celle du compte à supprimer. Cette signature électronique permet à Goodflag de s'assurer de l'identité et de l'accord du demandeur, qu'elle correspond bien au compte à supprimer et d'éviter toute tentative de suppression de preuve par une personne mal intentionnée. Goodflag s'engage à fournir un procès-verbal de destruction du compte Utilisateur mentionné dans un délai maximal d'un mois. Tout formulaire incomplet ne pourra pas être pris en compte par Goodflag.

5. Utilisation du Service par le Signataire

Le Signataire utilise le Service de manière unique en exécutant une Transaction qui lui permet de signer un ou plusieurs Document(s) d'un ou plusieurs Parapheur(s). Les paragraphes ci-dessous décrivent les différentes étapes d'une Transaction.

5.1 Réception d'un courriel contenant une invitation à signer

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.

5.2 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.

5.3 Présentation de la Page de consentement

La Page de consentement s'affiche dans le navigateur Internet du Signataire. Elle lui présente 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.

5.4 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).

5.5 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 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 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.

¹ Autrement dit, le Certificat qualifié est émis conformément à l'article 24, paragraphe 1, alinéa a, du Règlement eIDAS (« version 2 »).

² Autrement dit, le Certificat qualifié est émis conformément à l'article 24, paragraphe 1, alinéa c, du Règlement eIDAS (« version 2 »).

5.6 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 2 manières différentes.

5.6.1 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.

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.

La signature des présentes CGU emporte l'acceptation par le Signataire du Certificat généré.

5.6.2 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.

5.7 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.

5.8 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.

5.9 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.

6. Conservation des données

Le Service conserve :

- Les Documents constitutifs des Parapheurs ;
- Les données de traçabilité des Transactions de Signature électronique 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 sont cachetés électroniquement par GOODFLAG et sont conservés par le Service de manière à assurer leur intégrité et leur confidentialité.

Il incombe à l'Utilisateur de télécharger les Documents relatifs aux Parapheurs terminés ou archivés en application de la législation, des réglementations, ou des procédures des autorités administratives ou juridiques applicables. L'Utilisateur est libre de mettre à la disposition des Signataires d'un Parapheur le Dossier de Preuve qui lui est attaché.

Le Service conserve :

- Pendant **1 an** les Documents des Parapheurs à partir du passage à l'état terminé ou clôturé ;
- Pendant **3 mois** les Documents des Parapheurs à partir de la date de création pour les Parapheurs à l'état brouillon, démarré ou arrêté.
- Pendant **7 ans** les Dossiers de Preuve relatifs aux Parapheurs arrêtés et/ou terminés et/ou clôturés.

GOODFLAG se réserve la possibilité de raccourcir ces durées de conservation, les Utilisateurs seront informés par courriel préalablement à la modification pour leur permettre de télécharger les Parapheurs terminés et clôturés.

Si le Signataire l'estime nécessaire, il peut émettre une demande de remise de Dossier de Preuve dans les 7 ans suivant la Transaction considérée et selon la procédure décrite au chapitre 14.2.

7. Obligations de l'Utilisateur et du Signataire

Les Utilisateurs garantissent que toutes les informations indiquées sur leur Compte Utilisateur ainsi que dans les champs obligatoires sont exactes, complètes, vraies et à jour.

Les Signataires utilisent la Signature électronique du Service, lequel Service est conforme au Règlement eIDAS, afin de manifester leur consentement aux Documents signés lors de la Transaction. Ils reconnaissent également qu'ils ont reçu toutes les informations requises pour la Signature électronique des Documents qu'ils signent, et que la Signature électronique proposée par le Service est un procédé fiable d'identification garantissant le lien entre chaque Signataire et chaque Document signé, conformément aux dispositions de l'article 1367 du Code civil français.

Les Utilisateurs et Signataires reconnaissent et acceptent que les Documents signés ont la même force probante qu'un document écrit sur papier conformément aux dispositions de l'article 1366 du Code civil français et que

le Document signé pourra valablement être invoqué devant les juridictions compétentes en cas de litige entre les Parties.

Les Utilisateurs et Signataires :

- N'utiliseront 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 porteront pas atteinte au fonctionnement du Service ;
- Assureront la confidentialité du(des) code(s) confidentiel(s) qui lui est(ont) adressé(s).

Les Utilisateurs et Signataires :

- Sont seuls responsables de la conformité de l'utilisation qu'ils font du Service vis-à-vis des lois et réglementations en vigueur ;
- Sont seuls responsables de l'adéquation du Service à leurs besoins.

L'Utilisateur déclare et garantit en outre :

- Conserver la confidentialité des moyens d'authentification de son Compte Utilisateur ;
- Être le seul responsable du contenu proposé en Signature.

Le Signataire déclare et garantit en outre :

- 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 ;
- Être garant de l'exactitude et de toutes les informations communiquées au Service ;
- Ne pas signer le(s) Document(s) à travers la Page de consentement, dès lors qu'une compromission ou suspicion de compromission du Service est portée à sa connaissance.

8. Responsabilité de GOODFLAG

GOODFLAG s'engage à délivrer un Service conforme à la description contractuelle, aux critères énoncés à l'article L 224-25-14 du Code de la consommation et aux spécificités définies par l'article liminaire du Code de la consommation.

La garantie légale de conformité inclut les mises à jour nécessaires au maintien de la conformité du Service, ainsi que l'assistance à laquelle l'Utilisateur et le Signataire peuvent légitimement s'attendre, sans frais, en écrivant par courriel au support Goodflag Community à l'adresse support-at-goodflag.community, en veillant à remplacer « -at- » par le symbole « @ ».

GOODFLAG répond des défauts de conformité existant au moment de la délivrance du Service qui apparaissent dans un délai de deux ans à compter de celle-ci.

Ce délai de garantie s'applique sans préjudice des articles 2224 et suivants du Code civil, la prescription commençant à courir au jour de la connaissance du défaut de conformité par l'Utilisateur ou par le Signataire.

En cas de défaut de conformité, l'Utilisateur ou le Signataire peut exiger la mise en conformité du Service délivré sauf s'il s'agit d'un défaut de conformité mineur.

L'Utilisateur peut également suspendre son Compte Utilisateur jusqu'à ce que GOODFLAG ait satisfait aux obligations qui lui incombent au titre de la garantie légale de conformité, dans les conditions des articles 1219 et 1220 du Code civil sauf s'il s'agit d'un défaut de conformité mineur. L'Utilisateur peut également demander la suppression de son Compte Utilisateur à tout moment selon la procédure prévue au chapitre 4.

Il appartient à l'Utilisateur ou au Signataire de solliciter auprès de GOODFLAG la mise en conformité du Service qui doit intervenir sans retard injustifié.

L'Utilisateur s'engage à coopérer avec GOODFLAG afin de lui permettre de vérifier la cause d'un défaut de conformité éventuel.

Tout service mis en conformité dans le cadre de la garantie légale de conformité bénéficie d'une extension de cette garantie de six mois.

Il est précisé que la responsabilité de GOODFLAG ne saurait être engagée dans les cas suivants :

- Non-respect de la législation du pays dans lequel le Service est délivré, qu'il appartient à l'Utilisateur de vérifier avant de créer son Compte Utilisateur ;
- En cas de mauvaise utilisation, d'utilisation à des fins commerciales, d'accident ou de force majeure ;
- Refus d'installation par l'Utilisateur, dûment informé dans un délai raisonnable des mises à jour nécessaires au maintien de la conformité du Service.

Il est également précisé qu'il n'existe pas de niveau minimal de qualité du Service.

GOODFLAG ne peut être tenue pour responsable de l'inadéquation du Service aux besoins des Utilisateurs et Signataires.

GOODFLAG ne peut être tenue pour responsable des Documents soumis à Signature électronique ainsi que pour tout usage du Service qui ne serait pas conforme à sa destination.

9. Droit de rétractation

Compte tenu de la nature des services fournis, qui nécessitent une exécution immédiate, les commandes de Service passées par l'Utilisateur ne bénéficient pas du droit de rétractation prévu par la loi. L'Utilisateur et le Signataire reconnaissent donc expressément renoncer au bénéfice du droit de rétractation.

10. 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 et à l'Utilisateur 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.

11. Protection des données à caractère personnel

GOODFLAG met en œuvre des traitements de Données Personnelles afin de fournir le Service et plus particulièrement, de permettre au Signataire d'être identifié et authentifié et d'apposer sa Signature électronique sur le Document.

11.1 Données à caractère personnel des Signataires

11.1.1 Cas général

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 des données, GOODFLAG agit comme responsable de traitement.

A ce titre, GOODFLAG collecte, traite et héberge des données à caractère personnel afin de fournir un service de Signature électronique conforme à la réglementation en vigueur.

Les données à caractère personnel traitées sont collectées directement auprès du Signataire ou indirectement auprès de l'Utilisateur.

Le tableau ci-dessous précise les Données Personnelles traitées, la finalité et la base légale du traitement ainsi que la durée de conservation des données. En revanche, les données effectivement traitées dépendent du niveau de Signature électronique exigé par l'Utilisateur.

Donnée personnelle	Finalité	Fondement légal	Durée de conservation
Nom de famille	Identification du Signataire et enregistrement dans le Dossier de Preuve	Intérêt légitime, nécessaire au service	7 ans dans le Dossier de Preuve
Prénom(s)	Identification du Signataire et enregistrement dans le Dossier de Preuve	Intérêt légitime, nécessaire au service	7 ans dans le Dossier de Preuve
Pays de naissance, nationalité ou pays de délivrance de la pièce d'identité vérifiée	Identification du Signataire et enregistrement dans le Dossier de Preuve	Intérêt légitime, nécessaire au service	7 ans dans le Dossier de Preuve

Donnée personnelle	Finalité	Fondement légal	Durée de conservation
Adresse courriel	Envoi d'un OTP courriel pour la Signature en mode Serveur afin d'authentifier le Signataire et enregistrement dans le Dossier de Preuve	Intérêt légitime, nécessaire au service	7 ans dans le Dossier de Preuve
Numéro de portable	Envoi d'un OTP SMS pour la Signature en mode Serveur afin d'authentifier le Signataire et enregistrement dans le Dossier de Preuve	Intérêt légitime, nécessaire au service	7 ans dans le Dossier de Preuve
Adresse IP	Enregistrement dans le Dossier de Preuve	Intérêt légitime, nécessaire au service	7 ans dans le Dossier de Preuve
Autres données pouvant se trouver dans un Jeton d'Identité (comme la date de naissance par exemple)	Vérification de l'identité du Signataire et enregistrement dans le Dossier de Preuve	Intérêt légitime, nécessaire au service	7 ans dans le Dossier de Preuve

GOODFLAG s'engage à ne pas divulguer à des tiers autres que ses [sous-traitants](#), des tribunaux (à des fins juridiques) ou autorités compétentes, les Données Personnelles relatives à chaque Signataire sans l'autorisation préalable de la personne concernée. Le Dossier de Preuve relatif à un Parapheur peut être téléchargé par l'Utilisateur qui l'a créé. La communication du Dossier de Preuve d'un Parapheur peut être demandée par tout Signataire de ce Parapheur par le biais d'un formulaire téléchargeable en cliquant sur ce [lien](#).

Toute opposition du Signataire à la conservation de ses données Personnelles empêche la délivrance d'un Certificat et la création de Signature. Le Signataire peut communiquer à GOODFLAG toute demande d'accès à ces Données Personnelles à l'adresse courriel dpo-at-goodflag.community après avoir pris soin d'avoir remplacé les caractères « -at- » par le symbole « @ ».

La Politique de confidentialité de GOODFLAG est accessible [ici](#).

11.1.2 Aspects propres à la Signature électronique avancée

En cas de signature électronique avancée avec authentification par SMS ou par courriel, l'Utilisateur a l'obligation de vérifier la pièce d'identité du Signataire. Cette opération génère un nouveau traitement de Données Personnelles ayant pour finalité la vérification de la pièce d'identité du Signataire.

Dès lors, l'Utilisateur est seul responsable de ce traitement de Données Personnelles. GOODFLAG ne peut être tenu responsable de l'usage qu'il sera fait de la pièce d'identité ou de sa durée de conservation.

11.1.3 Aspects propres à la Signature qualifiée

La Signature qualifiée repose sur un Certificat qualifié qui nécessite une authentification :

- Via 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 », 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 ; autrement dit, le Certificat qualifié est émis conformément à l'article 24, paragraphe 1, alinéa a, du Règlement eIDAS (« version 2 ») ;
- Via 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 conformité, 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 ; autrement dit, le Certificat qualifié est émis conformément à l'article 24, paragraphe 1, alinéa c, du Règlement eIDAS (« version 2 »).

Dans ce cadre-là uniquement, le moyen d'identification agit comme sous-traitant de GOODFLAG, toute demande relative à la protection des données doit être adressée en priorité à GOODFLAG.

11.2 Données à caractère personnel de l'Utilisateur

Goodflag met en œuvre les traitements de Données à caractère personnel conformément à sa Politique de confidentialité disponible [ici](#).

12. Confidentialité

GOODFLAG prendra toutes les mesures nécessaires pour protéger les informations confidentielles échangées sur le Service.

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

13. 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 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 est le titulaire.

14. Effets juridiques et convention de preuve

14.1 Effets juridiques d'une Signature électronique

Tout contrat conclu par des moyens électroniques selon la procédure décrite dans les CGU est formé lorsque le Document porte la Signature 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 Electronique 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 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 soumis aux juridictions compétentes en cas de litige 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 avoir tout pouvoir pour signer au nom et pour le compte de ladite Partie.

Les Parties acceptent que :

- (i) Le Signataire manifeste son consentement selon le protocole décrit à l'article 4.3. des présentes CGU ;

- (ii) Les actions visées dans le (i) ci-dessus sont soumises aux juridictions compétentes en cas de litige et doivent faire 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 Electronique 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 pourront être soumis aux juridictions compétentes en cas de litige entre les Parties.

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

14.2 Le Dossier de Preuve

GOODFLAG conserve le Dossier de Preuve d'une signature pendant une durée de 7 ans. Cela signifie que dans le cas où un litige surviendrait au-delà de cette durée, GOODFLAG ne sera pas en mesure de produire le Dossier de Preuve correspondant. Le contenu du Dossier de Preuve est décrit dans le Cahier des fonctionnalités du Service dont le lien est fourni à l'annexe 2. L'Utilisateur peut directement télécharger le Dossier de Preuve relatif à un Parapheur une fois celui-ci terminé. La communication du Dossier de Preuve peut être demandée par tout Signataire par le biais d'un formulaire accessible [ici](#).

Le Signataire doit signer le formulaire à l'aide d'une Signature électronique réalisée à l'aide du Service, l'adresse de courriel utilisée doit être la même que celle utilisée pour la Signature électronique pour laquelle le Dossier de Preuve est exigé.

Il est nécessaire pour le Signataire de fournir les informations suivantes :

- L'adresse de courriel de l'Utilisateur qui a créé le Parapheur pour lequel il est demandé le Dossier de Preuve ;
- Le nom du Parapheur objet de la demande de Dossier de Preuve ;
- La date (année - mois - jour) et l'heure (heures - minutes) de création du Parapheur objet de la demande de Signature.

15. Contact

Pour toute réclamation ou question sur l'utilisation et le fonctionnement du Service, le Signataire peut a) contacter l'Utilisateur qui lui a soumis un Parapheur avec le(s) Document(s) à signer ainsi que b) contacter le

support Goodflag Community à l'adresse support-at-goodflag.community, en veillant à remplacer « -at- » par le symbole « @ ».

16. Mentions Légales

Le site Internet du Service est détenu et exploité par GOODFLAG, société par actions simplifiée dont siège social est sis 9, avenue du Maréchal Leclerc - 10120 St-André-les-Vergers, immatriculée au Registre du Commerce et des Sociétés de Troyes sous le numéro 480 622 257.

Le directeur de la publication du site Internet www.goodflag.community est M. François Devoret.

17. Hébergement

Le site Internet www.goodflag.community est hébergé par les sociétés Hexanet et Celeste respectivement au 3 Allée Albert Caquot, 51100 Reims et 20 Rue Albert Einstein, 77420 Champs-sur-Marne.

18. Force majeure

Les Parties ne pourront être tenues pour responsables si la non-exécution ou le retard dans l'exécution de l'une quelconque de leurs obligations, telles que décrites dans les présentes découle d'un cas de force majeure, au sens de l'article 1218 du Code civil.

19. Droit applicable – Langue

Les présentes CGU et les opérations qui en découlent sont régies par le droit français.

Elles sont rédigées en langue française. Dans le cas où elles seraient traduites en une ou plusieurs langues, seul le texte français ferait foi en cas de litige.

20. Litiges

Tous les litiges auxquels les opérations d'achat et de vente conclues en application des présentes conditions générales de vente pourraient donner lieu, concernant tant leur validité, leur interprétation, leur exécution, leur résiliation, leurs conséquences et leurs suites et qui n'auraient pu être résolues entre Goodflag et l'Utilisateur seront soumis aux tribunaux compétents dans les conditions de droit commun.

L'Utilisateur et le Signataire sont informés qu'ils peuvent en tout état de cause recourir à une médiation conventionnelle, notamment auprès de la Commission de la médiation de la consommation (C. consom. art. L 612-1) ou auprès des instances de médiation sectorielles existantes dont les références figureraient sur le site Internet de Goodflag ou à tout mode alternatif de règlement des différends (conciliation, par exemple) en cas de contestation.

L'Utilisateur, constatant qu'une violation au règlement général sur la protection des données personnelles aurait été commise, a la possibilité de mandater une association ou un organisme mentionné au IV de l'article 43 ter de la loi informatique et liberté de 1978, afin d'obtenir contre le responsable de traitement ou sous-traitant, réparation devant une juridiction civile ou administrative ou devant la commission nationale de l'informatique et des libertés.

21. Attribution de la conception du Site Internet et coordonnées de l'éditeur

LEX PERSONA (GOODFLAG), société par actions simplifiée dont siège social est sis 9, avenue du Maréchal Leclerc – 10120 St-André-les-Vergers, immatriculée au Registre du Commerce et des Sociétés de Troyes sous le numéro 480 622 257. Contact : <https://www.goodflag.com/contact>.

22. Annexe 1

Les Conditions Générales d'Utilisation des Certificats délivrés par l'AC « Sunnystamp Natural Persons CA » dans le cas d'une Signature en mode serveur avec Certificat à la volée mise en œuvre par le Service sont décrites ci-dessous.

Contact de l'AC	LEX PERSONA (GOODFLAG) 9 AVENUE MARECHAL LECLERC 10120 ST ANDRE LES VERGERS « a FRANCE Adresse courriel : pki-at-sunnystamp.com (remplacer « -at- » par « @ ») 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 ici. 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 de 1 heure et ne peuvent être utilisés que pour signer les documents de la Transaction de Signature électronique pour laquelle ils ont été spécialement créés. Dans le cadre du présent Service, l'AC délivre 4 types de Certificats : • Les Certificats utilisés par ses répondants OCSP pour signer les Réponses OCSP ; • Les Certificats, identifiés par l'OID 1.3.6.1.4.1.22542.100.1.1.1.3 et appelés « Certificats OPEN REG », pour lesquels la PC/DPC laisse l'Autorité d'Enregistrement déléguer au Client le processus d'enregistrement appliqué pour authentifier et vérifier l'identité des Signataires ; • Les Certificats, identifiés par l'OID 1.3.6.1.4.1.22542.100.1.1.1.4 et appelés « Certificats FranceConnect », délivrés à la suite d'une authentification du Signataire par un Fournisseur d'identité proposé par FranceConnect ; • Les Certificats, identifiés par l'OID 1.3.6.1.4.1.22542.100.1.1.1.5 et appelés « Certificats MIE eIDAS », 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 : ◦ notifié conforme aux exigences énoncées à l'article 8 du règlement eIDAS version 2 en ce qui concerne le niveau de garantie « élevé »³ ; ou bien

³ Autrement dit, ces Certificats qualifiés sont émis conformément à l'article 24, paragraphe 1a, alinéa a, du règlement eIDAS v2.

	◦ qui permet d'identifier une personne physique avec un degré de confiance élevé et dont la conformité est confirmée par un organisme d'évaluation de la conformité⁴. Les Certificats sont émis par l'AC « Sunnystamp Natural Persons CA » qui est elle-même émise par l'AC racine « Sunnystamp Root CA G2 ». Les certificats de ces AC sont disponibles ici.
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	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. Validation de l'identité du Signataire : <u>Pour les Certificats OPEN REG :</u> Le Client doit fournir au minima à l'AE les nom et prénom(s) du Signataire devant signer les documents. 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. <u>Pour les Certificats FranceConnect :</u> Le Client doit fournir au minima à l'AE les nom et prénom(s) du Signataire devant signer les documents. L'AE délègue la validation de l'identité du Signataire à FranceConnect et récupère auprès de FranceConnect les informations d'identité suivantes du Signataire : • Nom de naissance ; • Prénom(s) ; • Date de naissance ; • Pays de naissance. <u>Pour les Certificats MIE eIDAS :</u> Le Client doit fournir au minima à l'AE les nom, prénom(s) du Signataire devant signer les documents.

⁴ Autrement dit, ces Certificats qualifiés sont émis conformément à l'article 24, paragraphe 1a, alinéa c, du règlement eIDAS v2.

	L'AE délègue la validation de l'identité du Signataire au MIE eIDAS et récupère auprès de celui-ci les informations d'identité suivantes du Signataire : • Nom de naissance ; • Prénom(s) ; • Date de naissance ; • Pays de naissance. Utilisation de la Clé Privée et du Certificat par le Signataire pour signer : La Clé Privée d'un Signataire est protégée par le Produit qui met en œuvre des moyens techniques et organisationnels pour garantir que seul le propriétaire de cette Clé Privée puisse l'utiliser pour signer. Dans le cas d'un Certificat FranceConnect ou MIE eIDAS, la Clé Privée du Signataire est générée et stockée sur un HSM certifié FIPS 140-2 level 3 ou équivalent.
Modalités de renouvellement	Il n'y a pas de processus de renouvellement.
Modalités de révocation	il n'y a pas de possibilité de révocation, dans la mesure où les Certificats sont générés à la volée pour une durée limitée à une heure dans le contexte d'une unique Transaction de Signature électronique qui s'exécute après avoir reçu le consentement de l'utilisateur.
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. L'AC ne peut être tenue responsable de l'utilisation du Certificat d'une manière non conforme à la PC/DPC. 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. 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.
Obligations des Signataires	Le Signataire à l'obligation de : • 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	Le Client à l'obligation de : • 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	Les UC ont l'obligation de : • 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.
Limite de responsabilité	Lex Persona (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. Lex Persona (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.
Références documentaires	La PC/DPC de l'AC est disponible ici .
Condition d'indemnisation	Sans objet.
Loi applicable et gestion des litiges	Les présentes CGU sont soumises au droit français. 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. 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.
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	L'AC est certifiée conforme à la norme ETSI EN 319 411-2 pour le niveau QCP pour les certificats émis selon la politique 1.3.6.1.4.1.22542.100.1.1.1.5. 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 ETSI EN 319 403.

23. Annexe 2

Le Cahier des fonctionnalités du Service est accessible [ici](#).