Goodflag Signature

Conditions Générales d'Utilisation du Service de Signature Electronique Qualifiée à Distance

Version 1.0

Date d'entrée en vigueur : 17/04/2026

OID du Service : 1.3.6.1.4.1.22542.100.3.1

9 Av Maréchal Leclerc – 10120 ST ANDRE LES VERGERS – FRANCE
Tél. : +33 (0)3 25 43 90 78 – www.goodflag.com
SAS au capital de 26 739 euros – R.C.S. Troyes 480 622 257 – Code APE 5829C – TVA FR01480622257

Table des matières

1. Introduction

1.1 Présentation générale

La société Lex Persona a adopté la marque commerciale Goodflag au début de l'année 2025. Dans les présentes Conditions Générales d'Utilisation (CGU), le nom Goodflag est utilisé en priorité dans la mesure où il s'agit de la marque principalement exposée aux Signataires ; Lex Persona demeure l'entité légale qui porte le service et, le cas échéant, les activités de prestataire de services de confiance qualifié au sens du règlement (UE) n° 910/2014.

Goodflag fournit un Service de Signature Électronique Qualifiée à Distance (SSEQAD) destiné aux personnes physiques. Ce service permet la création de signatures électroniques qualifiées à distance au moyen d'un dispositif qualifié de création de signature électronique (Qualified Signature Creation Device - QSCD) opéré dans un environnement contrôlé et sécurisé. Les présentes CGU s'adressent principalement aux Signataires, ainsi qu'aux personnes ou systèmes qui se fient aux signatures produites via le SSEQAD.

Le SSEQAD n'est pas un service de signature générique couvrant plusieurs niveaux de signature. Il est limité à la création de signatures électroniques qualifiées pour des personnes physiques. Les présentes CGU ne régissent ni les autres niveaux de signature, ni les modules ou applications tiers permettant d'initier une demande de signature, sauf mention expresse contraire.

1.2 Acceptation et opposabilité des CGU

Les CGU du SSEQAD, s'entendent au sens de la norme ETSI EN 319 401 (paragraphe 6.2) et sont établies conformément aux exigences de la norme ETSI TS 119 431-1 (paragraphe 4.3.3).

Les présentes CGU définissent les conditions d'utilisation du SSEQAD par les Signataires. Elles sont mises à disposition du Signataire avant l'entrée dans la relation contractuelle relative à l'utilisation du service et avant tout acte de signature. L'acceptation des CGU intervient dans le cadre du Parcours de Consentement, par une action explicite du Signataire. Cette acceptation vaut reconnaissance, par le Signataire, du caractère opposable des présentes CGU.

Les CGU sont communiquées au Signataire sous forme électronique. La version applicable est celle en vigueur à la date de l'utilisation du SSEQAD concernée.

1.3 Identification du document

Le présent document constitue les Conditions Générales d'Utilisation du SSEQAD opéré par Goodflag. Il est rattaché à l'OID 1.3.6.1.4.1.22542.100.3.1, qui identifie la politique et le corpus documentaire du SSEQAD correspondant. Toute évolution substantielle du présent document donne lieu à une nouvelle version et, le cas échéant, à une mise à jour des identifiants et références documentaires applicables.

2. Références normatives

Les présentes CGU s'inscrivent notamment dans le cadre des textes et normes suivants :

- Règlement (UE) n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (règlement eIDAS), ainsi que ses textes d'application et d'évolution ;

- ETSI EN 319 401, General Policy Requirements for Trust Service Providers ;
- ETSI EN 319 411-2, Policy and security requirements for Trust Service Providers issuing EU qualified certificates ;
- ETSI TS 119 431-1, Policy and security requirements for trust service providers supporting server signing ;
- Le cas échéant, les référentiels applicables aux prestataires de services de confiance qualifiés et aux dispositifs qualifiés de création de signature.

3. Politique applicable / documents de référence

Le SSEQAD est régi, en complément des présentes CGU, par les documents suivants, dans leur version en vigueur :

- La Politique de Service de Signature Électronique Qualifiée à Distance et sa Déclaration des Pratiques de Service associée (PSSEQAD/DPSSEQAD) ;
- La Politique Générale des Services de Confiance de Goodflag / Lex Persona (PGSC), pour les exigences transverses qu'elle définit ;
- La Politique de Certification et la Déclaration des Pratiques de Certification de l'Autorité de Certification « Sunnystamp Natural Persons CA » ;
- Les informations publiées dans le dépôt documentaire officiel de Goodflag / Lex Persona, y compris, le cas échéant, les Certificats d'AC, les informations de validation et les versions applicables des politiques.

En cas de contradiction entre les présentes CGU et les documents techniques ou contractuels applicables au service, l'interprétation se fait en cohérence avec le règlement eIDAS, les normes ETSI applicables et la PSSEQAD/DPSSEQAD, sous réserve des droits impératifs reconnus aux Signataires par la loi applicable.

4. Définitions

Autorité de Certification (AC) : entité qui, au sein d'un prestataire de services de confiance, émet et gère des Certificats. Dans le cadre du SSEQAD, l'AC utilisée pour l'émission des Certificats qualifiés de signature est « Sunnystamp Natural Persons CA ».

Autorité d'Enregistrement (AE) : entité chargée de l'identification des Signataires et de la gestion des demandes de Certificats ou des données nécessaires à leur émission.

Bi-clé : combinaison d'une clé privée et d'une clé publique utilisée pour effectuer des opérations cryptographiques.

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'AC 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'AC 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 de la présente PSSEQAD/DPSSEQAD, 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 Lex Persona et dédié à une Transaction.

Clé Privée : clé d'une Bi-clé destinée à rester sous le contrôle exclusif de son titulaire et utilisée pour créer la signature électronique.

Client : entité légale ayant contractualisé avec Goodflag afin d'utiliser le SSEQAD et de faire signer des documents à des Signataires.

Moyen d'Identification Électronique (MIE) : moyen d'identification électronique notifié au sens du règlement eIDAS, de niveau élevé, ou admis comme équivalent selon le cadre juridique applicable au service.

Parcours de Consentement : ensemble des interactions entre le SSEQAD et le Signataire au cours desquelles celui-ci consulte les documents, accepte les CGU, s'authentifie et confirme explicitement sa volonté de signer.

QSCD : dispositif qualifié de création de signature électronique au sein duquel la Clé Privée de signature est générée, protégée et utilisée sans quitter le dispositif.

SAD : données d'activation de signature permettant au Signataire d'autoriser l'opération de signature et au SSEQAD d'activer, sous contrôle logique approprié, l'utilisation de la Clé Privée dans le QSCD.

Signataire : personne physique identifiée qui utilise le SSEQAD pour signer un ou plusieurs document(s) dans le cadre d'une Transaction déterminée.

Transaction : opération déclenchée à l'initiative d'un Utilisateur habilité par le Client et ayant pour finalité la signature d'un ou plusieurs document(s) par un Signataire.

Utilisateur de Signature (US) : personne physique ou morale, ou système applicatif, qui se fie à une signature produite par le SSEQAD pour vérifier l'intégrité d'un document signé et l'identité du Signataire.

5. Acronymes

AC	Autorité de Certification
AE	Autorité d'Enregistrement
CGU	Conditions Générales d'Utilisation
DPSSEQAD	Déclaration des Pratiques du Service de Signature Électronique Qualifiée à Distance
HSM	Hardware Security Module
MIE	Moyen d'Identification Électronique
OID	Object Identifier
PSSEQAD	Politique de Service de Signature Électronique Qualifiée à Distance
QSCD	Qualified Signature Creation Device

SAD	Signature Activation Data
SAM	Signature Activation Module
SSEQAD	Service de Signature Électronique Qualifiée à Distance
US	Utilisateur de Signature

6. Politique de service appliquée

Le SSEQAD est fourni conformément à la politique de service identifiée par l'OID 1.3.6.1.4.1.22542.100.3.1. Cette politique encadre la création de signatures électroniques qualifiées à distance pour des personnes physiques, au moyen d'un QSCD distant, dans le respect de la PSSEQAD / DPSSEQAD et des normes ETSI et EN applicables.

Le SSEQAD s'appuie sur l'émission, à la volée, d'un Certificat qualifié de signature lié à une Bi-clé éphémère générée dans le QSCD pour la seule durée de la Transaction. Le Certificat qualifié correspondant est émis par l'AC « Sunnystamp Natural Persons CA » pour une durée de validité maximale d'une heure. La Bi-clé associée est détruite à l'issue de la Transaction ou en cas d'échec, d'interruption ou d'expiration.

Le Signataire est authentifié au moyen d'un MIE conforme aux exigences applicables au service. Le SSEQAD ne permet pas au Signataire d'accéder directement à sa Clé Privée ; il garantit que l'utilisation de celle-ci demeure confinée au QSCD et ne peut intervenir qu'après réalisation des contrôles prévus, dont l'acceptation des CGU, l'authentification et l'expression explicite de la volonté de signer.

Les présentes CGU sont spécifiques au SSEQAD. Elles ne valent pas, sauf stipulation expresse, pour d'autres services de confiance, pour d'autres niveaux de signature ou pour des services d'orchestration applicative extérieurs au périmètre du SSEQAD.

7. Limitations d'usage du service

Le SSEQAD ne peut être utilisé que pour la création de signatures électroniques qualifiées de personnes physiques dans le cadre d'une Transaction déterminée. Il ne peut pas être utilisé pour créer des signatures simples ou des signatures avancées qui sont hors périmètre du SSEQAD, ou pour réaliser des opérations cryptographiques autres que celles prévues par les présentes CGU et les politiques applicables.

Le Certificat qualifié émis à la volée dans le cadre du SSEQAD ne peut être utilisé que pour signer les documents de la Transaction pour laquelle il a été créé. Sa durée de validité maximale est d'une heure et il n'a pas vocation à être réutilisé au-delà de cette Transaction. De même, la Clé Privée associée est éphémère, non exportable, non duplicable, non sauvegardée et non accessible directement au Signataire.

La signature produite par le SSEQAD ne porte que sur les documents dont l'empreinte SHA 256 a été intégrée à la Transaction. Les pièces jointes non soumises à signature, les documents non présentés dans le Parcours de Consentement ou les contenus modifiés après la signature ne bénéficient pas de la signature qualifiée créée au titre de la Transaction.

Le Signataire ne doit pas utiliser le SSEQAD dans un contexte illicite, frauduleux ou contraire aux lois et règlements applicables. Le service ne dispense pas le Client, le Signataire ou l'US de vérifier l'adéquation juridique de l'acte signé à son contexte métier ou réglementaire.

Sous réserve des limitations légales applicables, les dommages résultant d'un usage du service au-delà des limitations prévues par les présentes CGU, par la politique de service ou par la politique de certification applicable ne sont pas couverts par les engagements de Goodflag.

8. Obligations du Signataire

Le Signataire s'engage à n'utiliser le SSEQAD qu'en ayant pleinement conscience de la portée juridique potentielle de sa signature électronique qualifiée, laquelle bénéficie en principe d'un effet juridique équivalent à celui d'une signature manuscrite dans les conditions prévues par le règlement eIDAS et le droit applicable.

Le Signataire s'engage notamment à :

- Prendre connaissance des présentes CGU avant de les accepter et ne pas poursuivre le Parcours de Consentement s'il ne les accepte pas ;
- Vérifier, avant de signer, le contenu des documents présentés ainsi que, le cas échéant, les informations d'identité affichées dans le Parcours de Consentement ;
- Utiliser personnellement le MIE ou tout autre moyen d'authentification admis dans le cadre du service, et en préserver la confidentialité et la sécurité ;
- Ne pas contourner les mécanismes d'identification, d'authentification, d'activation ou de sécurité du SSEQAD ;
- Fournir, directement ou indirectement par l'intermédiaire du Client ou de l'Utilisateur habilité, des informations exactes, sincères et à jour ;
- Signaler sans délai au Client ou à Goodflag toute anomalie, erreur manifeste, dysfonctionnement ou suspicion d'usage frauduleux affectant la Transaction ou le service ;
- Utiliser le SSEQAD conformément aux lois et règlements applicables, ainsi qu'aux instructions légitimes communiquées dans le Parcours de Consentement.

Le Signataire demeure responsable de l'usage des moyens d'authentification placés sous son contrôle. Toute défaillance imputable à une mauvaise utilisation de ces moyens, à leur compromission du fait du Signataire ou à des informations erronées fournies au service peut affecter la possibilité de signer, la délivrance du Certificat qualifié ou l'opposabilité des éléments techniques associés.

9. Informations destinées aux Utilisateurs de Signature et autres parties se fiant au service

Les US et, plus généralement, les parties qui se fient aux signatures produites via le SSEQAD doivent vérifier la signature électronique, le Certificat qualifié associé, la chaîne de certification et les informations de confiance publiées par Goodflag / Lex Persona ou par les AC concernées, au moyen d'outils et de procédures adaptés.

Compte tenu du caractère éphémère du Certificat qualifié émis à la volée pour le Signataire, sa période de validité est limitée dans le temps. L'US doit en tenir compte lors de la vérification des signatures. La vérification doit porter, a minima, sur l'intégrité du document signé, la validité du

Certificat à la date de la signature, la chaîne de certification applicable et, le cas échéant, les informations de confiance et d'horodatage associées.

Les US doivent respecter les limitations d'usage du Certificat et de la signature produite. Une confiance accordée au-delà du périmètre fonctionnel ou temporel décrit dans les présentes CGU, dans la politique de service ou dans les politiques de certification applicables relève de la responsabilité de la partie qui s'y fie.

Les informations nécessaires à la vérification des Certificats et des signatures, y compris les politiques applicables et les Certificats d'autorité pertinents, sont publiées dans le dépôt officiel de Goodflag / Lex Persona ou rendues disponibles par les moyens prévus par les politiques de certification applicables.

10. Durée de conservation des journaux d'événements

Le SSEQAD journalise les événements nécessaires à la sécurité, à la traçabilité et à la valeur probante des opérations réalisées, notamment les identifiants techniques de Transaction, les horodatages, les résultats des contrôles, la référence du Certificat, ainsi que les événements significatifs intervenant lors de l'identification, de l'authentification, de l'activation et de l'exécution de la Transaction de signature.

Les journaux d'événements sont conservés pendant une durée compatible avec les exigences réglementaires, normatives et contractuelles applicables au service. Les dossiers de preuve relatifs aux Transactions sont, sauf conditions particulières, conservés pendant dix ans. La durée de conservation calendaire applicable aux journaux d'événements techniques du SSEQAD est fixée dans le corpus documentaire interne et dans les politiques applicables.

Pendant leur durée de conservation, les journaux et éléments probants font l'objet de mesures destinées à préserver leur intégrité, leur confidentialité et leur disponibilité, conformément au corpus de sécurité applicable au SSEQAD.

Goodflag conserve les données d'audit 10 ans.

11. Limitations de responsabilité

Goodflag assume, en tant que prestataire de services de confiance qualifié lorsque le cadre juridique l'exige, les responsabilités qui lui incombent en application du règlement eIDAS, du droit français applicable et des textes pris pour leur application. Les présentes CGU ne limitent pas les responsabilités impératives auxquelles il ne peut être légalement dérogé.

Sous réserve des dispositions d'ordre public applicables, Goodflag ne saurait être tenue responsable :

- D'une utilisation du SSEQAD, du Certificat qualifié ou des informations de validation en dehors du périmètre, de l'objet ou de la durée pour lesquels ils ont été prévus ;
- Des conséquences d'informations erronées, incomplètes ou obsolètes fournies par le Client, l'Utilisateur habilité ou le Signataire ;
- De l'indisponibilité ou du dysfonctionnement de moyens d'authentification, de réseaux de communication ou de services tiers extérieurs au périmètre de responsabilité de Goodflag ;

- Des dommages indirects, pertes d'exploitation, pertes de chance, pertes financières ou pertes de données qui ne résultent pas directement d'un manquement démontré de Goodflag à ses obligations légales ou contractuelles ;
- De la confiance accordée par un US ou une autre partie au-delà des limitations d'usage décrites dans les présentes CGU et dans les politiques applicables.

Le Signataire demeure responsable de l'usage de ses moyens d'authentification, du contrôle qu'il exerce sur sa volonté de signer et, plus généralement, du respect de ses propres obligations. Les limitations du présent article ne s'appliquent pas en cas de dol, de faute lourde ou lorsqu'une telle limitation est interdite par la loi applicable.

12. Droit applicable

Les présentes CGU sont soumises au droit français, sous réserve des règles impératives plus protectrices éventuellement applicables au Signataire lorsqu'elles ne peuvent être écartées par convention.

Les effets juridiques de la signature électronique qualifiée, les obligations relatives au service de confiance et les conditions de preuve sont appréciés conformément au règlement eIDAS, aux normes applicables et au droit français.

13. Plaintes et règlement des litiges

Toute réclamation relative à l'utilisation du SSEQAD, au déroulement d'une Transaction, à l'émission d'un Certificat qualifié dans le cadre du service, ou à l'application des présentes CGU peut être adressée en premier lieu au support du Client qui a soumis les documents à signer, lorsqu'il est l'interlocuteur opérationnel du Signataire.

Lorsque la réclamation porte directement sur le fonctionnement du SSEQAD, sur la délivrance des Certificats qualifiés ou sur les engagements relevant de Goodflag / Lex Persona, elle peut également être adressée à Goodflag par les moyens de contact indiqués à l'article 15. Goodflag met en œuvre une procédure interne de traitement des plaintes et réclamations.

En cas de litige, les parties s'efforcent de rechercher une solution amiable. A défaut de règlement amiable, en cas de litige relatif à l'interprétation, la formation, la validité ou le respect des présentes CGU, et faute d'être parvenus à un accord ou à une transaction dans un délai d'un (1) mois à compter de l'apparition du différend, les Parties donnent compétence expresse et exclusive aux Tribunaux de Troyes, nonobstant pluralité de défendeurs, d'action en référé ou d'appel en garantie ou de mesure conservatoire.

14. Évaluation de conformité et schéma d'évaluation

Le SSEQAD relève d'un cadre normatif fondé notamment sur le règlement eIDAS, ETSI EN 319 401, ETSI EN 319 411-2 et ETSI TS 119 431-1. Lorsqu'il est présenté comme service de confiance qualifié ou lorsqu'une évaluation de conformité est requise, le service est destiné à être évalué ou est évalué selon le schéma de conformité applicable aux prestataires de services de confiance, par un organisme d'évaluation compétent et selon les référentiels en vigueur.

L'état de conformité du SSEQAD et le schéma d'évaluation effectivement appliqué sont indiqués dans la documentation de conformité mise à disposition par Goodflag / Lex Persona, le cas échéant dans son dépôt documentaire officiel, disponible sur le site de Goodflag / Lex Persona.

Lorsqu'une conformité a été évaluée, cette évaluation ne vaut que dans les limites du périmètre, de la version du service et du schéma d'évaluation concernés.

15. Coordonnées de contact

Les coordonnées de contact de Goodflag / Lex Persona pour les questions relatives au SSEQAD sont les suivantes :

Goodflag / Lex Persona
9, avenue Maréchal Leclerc
10120 Saint-André-les-Vergers
France
Courriel : pki-at-sunnystamp.com (remplacer les caractères « -at- » par « @ »)
Téléphone : +33 (0)3 25 43 90 78
Site de publication / repository : https://pki2.sunnystamp.com/repository

16. Engagements de disponibilité

Le SSEQAD est fourni avec un objectif de disponibilité compatible avec sa finalité de service de confiance. Sauf engagement particulier convenu avec le Client, le service est accessible en ligne vingt-quatre heures sur vingt-quatre et sept jours sur sept, hors cas de force majeure, opérations de maintenance, mises à jour, incidents de sécurité, défaillances de réseaux ou indisponibilités imputables à des services tiers ou à des composants extérieurs au périmètre de responsabilité de Goodflag.

Goodflag peut interrompre ou limiter temporairement l'accès au SSEQAD lorsque cela est nécessaire pour préserver la sécurité, l'intégrité, la confidentialité, la conformité ou la continuité du service. Lorsque les circonstances le permettent, une information appropriée est communiquée aux parties concernées.

Sauf stipulation expresse contraire, les présentes CGU ne constituent pas un engagement de niveau de service individualisé au bénéfice du Signataire.

17. Protection des données à caractère personnel

Dans le cadre du SSEQAD, Goodflag traite des données à caractère personnel nécessaires à l'identification et à l'authentification du Signataire, à la création de la signature électronique qualifiée, à la constitution du dossier de preuve, à la conservation des éléments probants et au respect des obligations légales et réglementaires applicables.

Selon les traitements concernés, Goodflag intervient soit en qualité de responsable de traitement, soit en qualité de sous-traitant pour le compte du Client, conformément au rôle réellement exercé pour l'opération considérée. Les données sont traitées conformément au règlement (UE) 2016/679 (RGPD), à la législation nationale applicable et au corpus documentaire de Goodflag relatif à la protection des données personnelles.

Le refus de fournir certaines données nécessaires à l'identification, à l'authentification ou à la preuve peut empêcher la poursuite de la Transaction, la délivrance du Certificat qualifié ou la création de la signature. Les personnes concernées peuvent exercer leurs droits auprès du Client lorsque celui-ci détermine les finalités du traitement, ou auprès de Goodflag selon les modalités d'information qui leur sont communiquées. Les coordonnées du délégué à la protection des données de Goodflag / Lex Persona sont dpo-at-goodflag.com (remplacer les caractères « -at- » par « @ »).

18. Confidentialité

Goodflag met en œuvre les mesures nécessaires pour protéger la confidentialité des informations dont il a la charge dans le cadre du SSEQAD. Sont notamment considérés comme confidentiels, sous réserve de leur nature et des obligations légales de publication, les journaux d'événements, les éléments de preuve, les données d'activation, les procédures internes de sécurité et les dossiers d'enregistrement associés au service.

Ne sont pas considérées comme confidentielles les informations qui doivent être publiées en application des textes, des normes ou des politiques applicables, notamment celles nécessaires à la vérification des Certificats et des signatures.

19. Sécurité

Le SSEQAD s'appuie sur un ensemble de mesures techniques et organisationnelles destinées à assurer la sécurité des opérations de signature, notamment la génération et l'utilisation des Clés Privées exclusivement dans un QSCD, la non-exportation des Clés Privées, la mise en œuvre de données d'activation, la journalisation des événements sensibles, la protection des communications, le cloisonnement des environnements, ainsi que les mécanismes de supervision, de détection d'anomalies et de traitement des incidents.

Le module d'activation de signature (SAM) utilisé dans le cadre du SSEQAD ne constitue pas lui-même un QSCD, mais il est exploité dans un environnement de sécurité destiné à garantir que l'activation de la signature ne peut intervenir qu'après authentification, contrôle de cohérence et expression explicite de la volonté du Signataire. La signature est créée exclusivement dans le QSCD.

Le Signataire reconnaît qu'Internet et les réseaux de communication peuvent présenter des risques résiduels. Il lui appartient de mettre en œuvre, sur ses propres équipements, les mesures de sécurité appropriées pour protéger son environnement, ses données et ses moyens d'authentification.

20. Effets juridiques et convention de preuve

La signature électronique qualifiée créée via le SSEQAD bénéficie, dans les conditions prévues par le règlement eIDAS et le droit applicable, d'un effet juridique équivalent à celui d'une signature manuscrite. Elle ne peut être refusée comme preuve en justice au seul motif qu'elle se présente sous forme électronique.

Les parties reconnaissent la valeur probante des journaux, éléments techniques, Certificats, horodatages, dossiers de preuve et autres données générés ou conservés dans le cadre du SSEQAD, sous réserve de l'appréciation souveraine des juridictions compétentes. Ces éléments ont vocation

à établir, notamment, l'identité du Signataire, le déroulement de la Transaction, l'acceptation des CGU, l'authentification, l'acte de signature et l'intégrité des documents signés.

Le recours au SSEQAD n'a pas pour effet de modifier les règles de validité matérielle des actes signés, ni les exigences substantielles éventuellement applicables aux documents concernés en vertu de textes spécifiques.

21. Dispositions finales

Si l'une quelconque des dispositions des présentes CGU était déclarée nulle, invalide ou inopposable, les autres stipulations demeureraient en vigueur, sauf si l'économie générale du document s'en trouvait affectée.

Goodflag peut faire évoluer les présentes CGU pour tenir compte d'une évolution du service, du cadre légal, réglementaire ou normatif, ou de ses pratiques documentées. Toute nouvelle version entre en vigueur à la date qu'elle indique et devient applicable aux utilisations postérieures du SSEQAD. Les présentes CGU sont rédigées en langue française. Elles peuvent être communiquées par voie électronique et conservées sur support durable.