OBJET DU DOCUMENT

Ce document a pour objet de fixer les Conditions Générales de fourniture par ISILIS - Société par Actions Simplifiée au capital de 308 387 Euros, située au 21-23 rue de Vienne, 75008 - Paris, immatriculée au RCS de Nanterre sous le numéro 452 818 958 - au Client de prestations visant à lutter contre la fraude à l'IBAN à travers le Logiciel IBANSecure.

La souscription par le Client à IBANSecure sur le site www.IBANSecure.fr emporte de plein droit acceptation expresse et sans réserve des présentes Conditions Générales par le Client. Elles prévalent sur tous autres documents commerciaux, y compris les conditions générales d'achat du Client.

Si une ou plusieurs stipulations des présentes CGV sont tenues non valides ou déclarées telles en application d'une loi, d'un règlement ou à la suite d'une décision définitive d'une juridiction compétente, les autres stipulations garderont toute leur force et leur portée.

Pour toute question relative aux fonctions disponibles à la date d'inscription ainsi qu'aux tarifs, adressez-vous au service commercial de IBANSecure : ibansecure@isilis.fr.

1 – LEXIQUE

Administrateur : Opérateur habilité à administrer le Logiciel IBANSecure pour le compte du Client

Banque émettrice : Banque partenaire d'ISILIS via laquelle les DDV seront émises sur le réseau SEPAmail DIAMOND.

Client : Entreprise utilisatrice du Logiciel IBANSecure durant une période limitée d'essai.

Conditions Générales : Désigne le présent document et ses annexes.

Demande de vérification (DDV) : Une demande de vérification correspond à un IBAN associé à une donnée identifiant une personne morale ou physique envoyé grâce à IBANSecure sur le réseau SEPAmail et dont le Client attend la confirmation de la correspondance, ou une réponse indiquant l'impossibilité de vérifier cette concordance

Heure / H : Heure exprimée en CET (Central European Time)

Identifiants bancaires : QXBAN et ICQX (identifiants bancaires SEPAmail DIAMOND)

Jour Ouvré : Jour ouvré du Lundi au Vendredi hors jours fériés français.

Logiciel : Le logiciel IBANSecure tel qu'il est décrit au sein du présent document ainsi que ses modules optionnels utilisés par le Client, accessible via l'interface web www.IBANSecure.fr.

SEPAmail DIAMOND : Service interbancaire permettant d'interroger la banque détentrice d'un compte afin qu'elle confirme l'identité du titulaire de ce compte. La liste des banques adhérentes au service est susceptible de changer et est disponible sur www.ibansecure.fr/BICReachable

2 - PERIODE D'ESSAI ET CONTRAT

Le Client s'inscrit librement à IBANSecure via l'interface web du Logiciel. Si un administrateur de la plateforme approuve son compte, il bénéficie automatiquement d'un essai d'une durée limitée déterminée au préalable d'un commun accord avec ISILIS permettant de tester le logiciel en mode démonstration.

ISILIS se réserve le droit de résilier tout essai d'un Client ayant déjà bénéficié d'une période de test gratuite et sans engagement.

3 - DESCRIPTION DU LOGICIEL

GENERALITES

Le Logiciel IBANSecure permet la fiabilisation des coordonnées bancaires des personnes physiques et personnes morales au travers du service interbancaire de validation SEPAmail Diamond.

PREREQUIS

Le Client devra disposer d'un identifiant bancaire SEPAmail Diamond (ICQX), pouvant si besoin être obtenu par ISILIS auprès de SEPAmail.

Le cas échéant, le Client devra fournir à ISILIS les informations nécessaires à l'obtention de son identifiant.

4 – CONDITIONS TARIFAIRES ET FACTURTION

A la souscription par le Client au Logiciel, ISILIS ouvrira la licence d'utilisation du Client lui permettant d'accéder au Logiciel.

Le Client souscrit un forfait de vérification valable pendant la période d'essai. Une facture sera émise à la création du forfait.

A l'issue de la période d'essai, les DDV qui n'auraient pas été consommées ne pourront ni être re-créditées, ni donner droit à un remboursement et le Client, s'il souhaite continuer à bénéficier du Logiciel devra signer un contrat avec ISILIS.

Par défaut le paiement devra être effectué par prélèvement.

Pour les paiements par virement, les factures relatives aux Prestations sont payables dans les trente (30) jours à compter de la date de facture, sans escompte, sauf à ce qu'il en soit stipulé autrement.

Dans le cas où le Client n'effectuerait pas le paiement dans les délais convenus, ISILIS pourra exiger de plein droit le paiement de pénalités de retard calculées au taux de trois (3) fois le taux d'intérêt légal en vigueur, majorées de 40€ forfaitaires à titre de frais administratifs de recouvrement.

5 – OBLIGATIONS D'ISILIS

En contrepartie du paiement du prix des prestations, ISILIS s'engage à :

- La disponibilité de ses données et des fonctionnalités du Logiciel, les Jours Ouvrés, de 9 heures à 12 heures et de 14 heures à 17 heures (CET), avec un temps de redémarrage en cas de panne de moins de quatre heures ouvrées ;
- Mettre en place les mesures de sécurité décrites en Annexe des CGV de manière à permettre le respect de la stricte confidentialité des données enregistrées dans la base de données d'IBANSecure ou échangées par le Client avec ses banques.

6 – OBLIGATIONS DU CLIENT

Le Client s'engage, à titre d'obligation essentielle, à payer à bonne date à ISILIS les sommes dues en contre partie de la réalisation des prestations par ISILIS, conformément aux modalités financières prévues aux présentes Conditions Générales.

Le Client s'engage à mettre au service d'ISILIS tous les moyens nécessaires à ce dernier pour lui faciliter l'exécution de ses obligations et s'engage à ne pas s'ingérer dans l'exécution technique de celles-ci.

Le Client informera également ISILIS, le cas échéant, de tout évènement ou modification susceptible d'avoir un impact sur la réalisation des Prestations.

Il est entendu qu'ISILIS ne sera tenu que par les documents et informations qui lui auront été préalablement transmis par le Client.

7 – CONDITIONS D'UTILISATION DU LOGICIEL IBANSECURE

Les données utilisées pour les vérifications (IBAN, SIREN, SIRET, n° de TVA pour une personne morale – IBAN, Nom Prénom, Date de naissance, Autre nom pour une personne physique) sont transmises aux banques pour vérification au travers du réseau interbancaire SEPAmail Diamond.

En utilisant IBANSecure, le Client s'engage à respecter les conditions d'utilisation de SEPAmail Diamond décrites ci-dessous.

Dans le cadre de la réalisation d'une demande de vérification (DDV) par le Client, ce dernier agit en tant que Donneur d'Ordre, c'est-à-dire celui qui demande la vérification d'un ou de plusieurs IBAN.

L'envoi d'une Demande de Vérification à IBANSecure suppose l'existence préalable ou en cours de création d'une relation d'affaires entre le Donneur d'Ordre et le Titulaire du compte à vérifier.

La Demande de Vérification devra obligatoirement contenir la référence du contrat existant entre le Donneur d'Ordre et le Titulaire du compte à vérifier, ou toute autre information permettant d'assurer une piste d'audit, en cas de réclamation du Titulaire du compte à vérifier.
La Demande de Vérification devra également obligatoirement contenir l'identifiant ICQX du Donneur d'Ordre. Ce dernier sera communiqué par IBANSecure au Client.
Par ailleurs, le Donneur d'Ordre s'engage à informer son client existant ou à venir du contrôle de cohérence qui pourra être réalisé sur les données bancaires qu'il lui aura communiquées.
ISILIS se réserve le droit de résilier de plein droit et sans mise en demeure préalable les présentes Conditions Générales en cas de non-respect par le Client des conditions d'utilisation du Logiciel IBANSECURE.

8 – PROPRIETE INTELLECTUELLE

ISILIS conserve l'entière propriété de ses droits d'auteur, dessins et modèles enregistrés, brevets, marques de commerce, logos, dessins et modèles (enregistrés ou non), droits sur les bases de données, secrets d'affaires et logiciels (en code source ou code objet).
ISILIS concède au Client une licence personnelle, mondiale, non exclusive, non transférable, sans le droit de concéder des sous-licences, révocable et limitée pour accéder à et utiliser les Services, ainsi que pour imprimer et faire des copies électroniques des rapports ou autres informations générés dans le cadre des Services.
Sont proscrits l'ingénierie inverse, la copie de tout ou partie du logiciel, la décompilation, le désassemblage du logiciel, le déchiffrage ou la modification du code source.

9 – RESPONSABILITE

ISILIS est responsable de l'acheminement des DDV auprès des banques. En revanche, sa responsabilité ne pourra être engagée si une banque ne répond pas aux DDV transmises pour quelque raison que ce soit ou si celle-ci répond de manière tardive.

L'envoi d'une DDV par le Client suppose l'existence préalable ou en cours de création d'une relation entre le Client et le titulaire du compte à valider. En conséquence, le Client s'interdit de faire usage du service à des fins de prospection commerciale. Le Client s'interdit également de mutualiser les résultats des DDV et de revendre ou redistribuer le résultat de cette mutualisation à des tiers.
Le Client déclare avoir effectué toute déclaration ou demande d'autorisation nécessaire relative à la mise en œuvre des traitements de données à caractère personnel, et s'engage à faire figurer toutes les mentions nécessaires permettant d'assurer l'information des personnes telle que prévue par la législation applicable relative au traitement des données à caractère personnel.
Par ailleurs, la responsabilité d'ISILIS ne saurait être engagée en cas de non-disponibilité du service bancaire pour quelque cause que ce soit ainsi qu'en cas de dysfonctionnements ou d'erreurs imputables à un tiers.
En outre, le Client ne pourra pas mettre en cause la responsabilité d'ISILIS dans les cas où celui-ci aurait respecté strictement les modalités des Prestations telles que décrites aux présentes et aurait exécuté l'intégralité des obligations lui incombant au titre des Conditions Générales ainsi que les instructions du Client.
De même, la responsabilité d'ISILIS ne saurait en aucun cas être recherchée lorsqu'une inexécution ou une mauvaise exécution qui lui est reprochée résulte d'une faute du Client, notamment dans la transmission à ISILIS des données, dans l'utilisation de ses logiciels, ou encore dans le non-respect des conseils donnés par ISILIS.
Le Client reconnait qu'il est le seul responsable de l'interprétation qu'il fait des résultats du contrôle qui lui sont communiqués. Il est précisé que l'utilisation du service ne permet pas au Client de bénéficier d'une garantie de bonne fin des opérations de paiement réalisées au moyen des coordonnées bancaires ayant fait l'objet d'une vérification et que les réponses obtenues dans le cadre du service ne sauraient dispenser leurs destinataires de procéder à des analyses complémentaires.
Notamment, concernant la vérification de comptes joints :

Le champ facultatif "Autre nom / prénom" ne peut en aucun cas être utilisé pour vérifier le nom d'un prétendu deuxième titulaire du compte. Ce champ ne peut servir qu'à vérifier l'autre nom (nom marital, nom d'usage) du même titulaire désigné dans le champ obligatoire « Nom/prénom »

Dans le cas où le champ "Autre nom" a été renseigné avec le nom d'un prétendu deuxième titulaire, les résultats Diamond ne sont pas exploitables. Nous déclinons alors toute responsabilité quant à une mauvaise interprétation des résultats faisant suite à une saisie erronée du champ « Autre Nom/prénom ».

Ainsi, dans le cas d'un compte joint, une DDV ne peut servir qu'à vérifier que l'IBAN appartient bien à l'un des deux titulaires. Pour vérifier les deux titulaires, il faudra donc réaliser deux DDV.

Toute réclamation relative à l'exécution des prestations objet des présentes devra être adressée à ISILIS par écrit dans un délai de huit (8) jours après l'achèvement de la prestation en cause. A défaut, la prestation sera réputée avoir été exécutée conformément aux demandes du Client.
En tout état de cause, et sauf en cas de faute lourde, la responsabilité d'ISILIS ne pourra être engagée pour un montant excédant un (1) mois moyen de facturation (sur la base des 12 derniers mois).
Il est entendu qu'ISILIS ne sera tenu qu'à la réparation des dommages matériels strictement consécutifs à sa défaillance, et dans les limites ci-dessus énoncées.
Le Client ne pourra donc en aucun cas réclamer la réparation d'un préjudice indirect et/ou immatériel découlant notamment mais non exclusivement de sa perte d'exploitation, de son préjudice commercial, de l'éventuelle baisse de son chiffre d'affaires, de la non-occurrence de l'impact commercial escompté, etc.
Dans tous les cas, ISILIS n'engage aucune responsabilité :

- Concernant le bien-fondé commercial, juridique ou financier des demandes de validation créés et envoyés par le Client ;
- Concernant la qualité des fichiers de données importés par le Client via Internet dans la base de données sur le serveur IBANSecure ;
- Concernant les conséquences des choix d'utilisation d'IBANSecure effectués par le Client quelles que soient les indications fournies par l'assistance technique ;
- Concernant le contenu des fichiers importés ou saisis par le Client dans IBANSecure ;
- Concernant la sécurité d'accès aux données du Client dès lors que cet accès est obtenu par la saisie normale du nom d'accès et du mot de passe choisis ;
- Concernant les réponses aux demandes de validations fournies par la banque émettrice du Client ou l'absence de réponses.
- Dans le cas d'opération sur un IBAN non vérifié via les présentes Conditions Générales et ce pour quelque cause que ce soit.

10 - FORCE MAJEURE

La survenance d'un cas de force majeure emportera suspension des obligations nées des présentes Conditions Générales, et exclusion de la responsabilité de la partie empêchée lorsque ses obligations sont rendues impossibles à réaliser, et ce jusqu'au rétablissement d'une situation normale. Aucune partie ne pourra être tenue responsable de retards ou de non exécutions résultant de causes échappant à son contrôle, et ce sans qu'il y ait faute ni négligence de la partie concernée.

Sont notamment considérés comme cas de force majeure, outre les cas habituellement retenus par les Cours d'Appel françaises et la Cour de Cassation, les évènements suivants : les grèves et conflits sociaux internes ou externes à l'entreprise, les épidémies et pandémies, l'impossibilité d'approvisionnement pour quelque raison que ce soit, les catastrophes naturelles et les évènements climatiques exceptionnels, les restrictions gouvernementales ou légales, les modifications légales ou réglementaires des formes de commercialisation, le blocage des télécommunications, du réseau, l'interruption de la fourniture d'énergie.

11 – CONFIDENTIALITE, PROPRIETE ET CONSERVATION DES DONNEES

CONFIDENTIALITE

Les parties s'engagent à respecter la confidentialité attachée aux informations qui leur sont communiquées, oralement ou par écrit, sous quelque forme que ce soit, dans le cadre de l'exécution des prestations, ci-après les « Informations Confidentielles ».

Il est convenu d'entendre par Information Confidentielle toute information échangée par les parties dans le cadre de la négociation, de la préparation, de la réalisation, ou de la fin des prestations, sans qu'il soit nécessaire que lesdites informations aient été désignées comme telles lors de leur communication à l'autre partie.

Les parties s'interdisent de divulguer ou de rendre accessible, directement ou indirectement, de quelque manière que ce soit y compris par négligence et à quelque personne que ce soit, tout ou partie des Informations Confidentielles sans l'accord exprès et préalable de l'autre partie.

Elles s'engagent notamment à ce titre à apporter au minimum le même niveau de protection aux Informations Confidentielles reçues qu'aux informations leur appartenant.

Les parties s'engagent également à porter à la connaissance de leur personnel ainsi qu'à leur(s) sous-traitant(s) éventuel(s) les obligations de confidentialité auxquelles elles sont tenues, et à prendre toute mesure nécessaire au respect de ces obligations.

Chaque partie avertira sans délai l'autre partie de toute violation de l'obligation de confidentialité visée au présent article dont elle aurait à connaître.

Le présent article s'applique aux Informations Confidentielles communiquées pendant toute la durée des prestations et poursuivra ses effets pendant une période de cinq (5) ans à compter de la fin des prestations pour quelque cause que ce soit.

CHIFFREMENT DES DONNEES

La solution IBANSecure assure le chiffrement des données échangées via Internet entre le poste de l'Administrateur et des Utilisateurs et le serveur IBANSecure, dans les deux sens. Le protocole utilisé est le standard SSL/TLS (Transport Layer Security), intégré à la plupart des navigateurs Internet.

La clé de chiffrement utilisée par ISILIS est déposée auprès d'un organisme de certification de réputation internationale.

Les données du Client sont stockées sur des serveurs exploités dans un environnement protégé contre les intrusions.

ISILIS s'engage à ne faire aucun usage de ces données, et à en limiter strictement les manipulations à ce qui est indispensable pour en assurer la sauvegarde.

PROPRIETE DES DONNEES

Le Client reste seul propriétaire des données que son Administrateur et ses Utilisateurs enregistrent dans sa base de données IBANSecure. Si nécessaire et sur simple demande écrite du Client en cas de résiliation par l'une des parties, ISILIS restitue ses données au Client, sous un délai de deux mois maximum, sous forme de fichiers standard ASCII, composés d'enregistrements séparés par des sauts de ligne et composés eux-mêmes de champs séparés par des tabulations. Les données sont toutes écrites en clair dans le fichier restitué et la description détaillée de la structure de ce fichier est fournie par ISILIS.

DONNEES SIGNALETIQUES

Les données signalétiques des tiers sont conservées de façon illimitée dans la base de données. Seul le Client peut supprimer tout ou partie du référentiel qu'il aura enregistré dans la base de données.

12 – PROTECTION DES DONNEES PERSONNELLES

Pour les besoins du présent article, les termes suivants « données à caractère personnel », « délégué à la protection des données », « traiter/traitement », « responsable du traitement », « destinataire », « sous-traitant » et « transférer/transfert » ont la même signification que celle qui leur est donnée dans le 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 (le « RGPD »).

Chaque partie s'engage à se conformer à la règlementation applicable à la protection des données personnelles, incluant le Règlement général Européen de protection des données personnelles n° 2016-679 dit « RGPD » et la loi n°78-17 du 6 janvier 1978 dite « Informatique et Libertés » telle qu'applicable à la date des présentes (ci-après la Règlementation).

Dans le cadre de l'exécution des prestations, ISILIS est susceptible de traiter ou d'accéder à des données personnelles. ISILIS intervient donc en sous-traitant du Client lequel demeure en toute hypothèse responsable de traitement au sens de la Règlementation.

CARACTERISTIQUES DU TRAITEMENT

Les caractéristiques des traitements de données à caractère personnel effectués par ISILIS pour le compte du Client responsable du traitement, telles que l'objet, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, sont détaillées en Annexe n°1.

Obligations du sous-traitant

(i) Respect des instructions du Client et de la réglementation

Le sous-traitant s'engage à :

- Traiter les données uniquement pour les seules finalités qui font l'objet de la sous-traitance
- Traiter les données personnelles conformément aux instructions documentées du Client, à moins qu'ISILIS ne soit tenu d'y procéder en vertu du droit applicable aux Conditions Générales. Dans ce cas, ISILIS informera le Client de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs d'intérêt public.
- Le cas échéant, respecter la réglementation en matière de secret bancaire et/ou toute autre réglementation applicable aux données à caractère personnel traitées ;
- Informer dans les meilleurs délais le Client si une de ses instructions constitue une violation de la réglementation applicable en matière de protection des données à caractère personnel et suspendre l'exécution de ladite instruction jusqu'à confirmation ou modification de l'instruction par le Client;
- S'assurer que les personnes autorisées à accéder aux données à caractère personnel ont connaissance des instructions du Client et s'engagent à ne traiter les données à caractère personnel qui leur sont confiées que dans le respect de celles-ci ;

- Veiller à ce que les personnes autorisées à accéder aux données à caractère personnel pour la réalisation des prestations reçoivent la formation nécessaire en matière de protection des données à caractère personnel ;
- Désigner un délégué à la protection des données et communiquer le nom et les coordonnées de celui-ci au Client; (Amélie Saidi – 01 40 89 99 38 – dpo@isilis.fr)
- Ne pas concéder, louer, céder ou autrement communiquer à une autre personne, tout ou partie des données à caractère personnel, même à titre gratuit, ainsi que ne pas utiliser les données à caractère personnel à d'autres fins que celles prévues aux présentes Conditions Générales, notamment, pour tout usage de prospection commerciale, marketing et/ou autre ;
- Prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut.

(ii) Sécurité, confidentialité, violation et destruction des données

Le sous-traitant s'engage à :

- Mettre en œuvre les mesures de sécurité décrites en Annexe n°2 des présentes Conditions Générales de manière à préserver la confidentialité et la sécurité des données à caractère personnel, et notamment, empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés, et plus généralement, de manière à protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment, lorsque le traitement comporte des transmissions de données dans un réseau ;
- Notifier au Client toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance, notamment afin de permettre à celui-ci de se conformer à l'obligation de notification à la CNIL, telle que décrit dans l'article 33 du RGPD;
- Respecter les durées de conservation des données à caractère personnel, telles que spécifiées par le Client ;
- Selon le choix du Client, détruire toutes les données à caractère personnel ou les lui renvoyer au terme des présentes Conditions Générales et détruire les copies existantes, ainsi que lui communiquer la preuve de ces destructions.

(iii) Assistance et audit

Le sous-traitant s'engage à :

- Aider et collaborer avec le Client afin de l'assister dans le respect des obligations incombant à ce dernier, conformément à la réglementation applicable en matière de protection des données à caractère personnel. Le sous-traitant apporte l'assistance nécessaire au Client pour la réalisation des analyses d'impact relatives à la protection des données et pour la réalisation de la consultation préalable de l'autorité de contrôle, en lui fournissant toutes informations utiles ;
- Transmettre dans les cinq (5) jours ouvrés tout élément portant sur les données à caractère personnel traitées, afin de permettre au Client de s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits à l'adresse dpo@isilis.fr
- Mettre à disposition du Client toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans les présentes Conditions Générales et lui incombant en tant que sous-traitant et permettre la réalisation d'audit, y compris des inspections par le Client ou un autre auditeur non-concurrent qu'il aura mandaté et contribuer à ces audits, dans la limite d'un audit par an (sauf en cas d'incident de sécurité) et avec un délai de prévenance d'un mois

Sous-traitance ultérieure

Le sous-traitant s'engage à ne pas sous-traiter l'exécution des prestations sans l'accord préalable, écrit et spécifique du Client. Néanmoins, il est d'ores et déjà accepté par les parties qu'ISILIS pourra sous-traiter tout ou partie des prestations à une ou plusieurs sociétés du groupe d'ISILIS, sous réserve d'en informer préalablement le Client.
Le sous-traitant demeure en tout état de cause pleinement responsable, dans les conditions et limites de l'article « Responsabilité », de l'exécution par cet éventuel sous-traitant de second rang, des obligations lui incombant et s'engage à répercuter auprès de ses sous-traitants les engagements et obligations auxquels il est tenu au titre des présentes Conditions Générales.

Transferts de données à caractère personnel hors-UE

ISILIS s'engage à ne transférer aucune donnée personnelle en dehors du territoire de l'UE sans l'autorisation écrite et préalable du client. Dans l'hypothèse où ISILIS serait autorisé à transférer des données personnelles hors du territoire de l'Union Européenne, il s'engage à ce que de tels transferts soient encadrés par l'adhésion à une décision d'adéquation de la Commission Européenne, la conclusion de Clauses Contractuelles Types de la Commission Européenne ou toute autre garantie appropriée qui serait prévu à l'Article 46 du RGPD.
Néanmoins, si le sous-traitant était tenu de procéder à de tels transferts en vertu du droit applicable, il s'engage à informer immédiatement le Client, sauf impossibilité légale.

13 - ENTREE EN VIGUEUR DES CONDITIONS GENERALES DE VENTE

Pendant la période d'essai, les Conditions Générales publiées au jour de l'inscription, telles qu'elles auront été validées par le Client lors du processus d'inscription régissent la relation entre le Client et ISILIS pour l'utilisation du Logiciel.
Au-delà de la période d'essai, dans le cas où le Client souhaite s'abonner au Logiciel, les parties s'engagent à signer un contrat.

14 - DROIT APPLICABLE ET ELECTION DE DOMICILE

Pour l'exécution des présentes ainsi que de leurs suites, les parties font respectivement élection de domicile en leurs sièges sociaux.
Préalablement à toute action en justice, les parties conviennent de rechercher une solution amiable à leur litige. A cet effet, les parties conviennent de se réunir dans les trente (30) jours de la réception de la lettre recommandée avec accusé de réception adressé par la partie faisant état du différend.
En l'absence ou en cas d'échec d'une solution amiable ou d'un plan d'action expressément accepté par les parties précisant les solutions apportées et les délais de mise en œuvre, dans les quinze (15) jours suivant la réunion initiale des parties précisée à l'alinéa précédent, les parties pourront soumettre le litige et attribueront compétence expresse au Tribunal de Commerce de Paris.
Cette clause s'applique même en cas de référé, d'appel en garantie ou de pluralité de défendeurs.

ANNEXE 1 : Description du traitement faisant l'objet de la gestion déléguée (sous-traitance) et sous-traitants autorisés

DESCRIPTION DU TRAITEMENT FAISANT L'OBJET DE LA GESTION DELEGUEE

Le sous-traitant est autorisé à traiter pour le compte du Client responsable du traitement les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) : fiabilisation des coordonnées bancaires des personnes physiques et personnes morales
La nature des opérations réalisées sur les données est leur traitement afin de valider ou non l'identité du ou des titulaire(s) d'un IBAN
La ou les finalité(s) du traitement est de s'assurer de l'identité du ou des titulaire(s) d'un IBAN avant tout paiement ou encaissement vers cet IBAN.
Les données à caractère personnel traitées sont :

Pour la validation d'un IBAN de personne physique :

- IBAN
- Nom/prénom
- Date de naissance

Pour la validation d'un IBAN d'une entreprise :

- IBAN
- SIREN
- SIRET
- Numéro TVA

Les catégories de personnes concernées sont les clients ou fournisseurs du Responsable de traitement.
Pour l'exécution du service objet du présent contrat, le responsable de traitement met à la disposition du sous-traitant les informations nécessaires suivantes :

- IBAN
- Nom/prénom
- Date de naissance
- SIREN
- SIRET
- Numéro TVA

SOUS-TRAITANTS AUTORISES

Nom du sous-traitant	**Description du traitement**	**Localisation**
SAFEO	Hébergement	France (Datacenter Equinix)
Loïc Angibaud	Conseil et expertise	France (41100)

ANNEXE 2 : Sécurité et modalités de conservation des données

HEBERGEMENT ET CONSERVATION DES DONNEES

- L'application et toutes ses données sont conservées chez notre hébergeur SAFEO, sur des serveurs exploités dans un environnement protégé contre les intrusions et sont entièrement chiffrées et donc invisibles par l'hébergeur.
- SAFEO s'appuie sur les datacenters Equinix, qui disposent de l'ensemble des certifications ci-après :
  - ISO 27001
  - PCI-DSS
  - OHSAS 18001
  - ISO 9001
  - ISO 22301
  - ISO 50001
  - ISO 14001
  - HDA/HADS
- Utilisation d'un proxy afin que la machine hébergeant l'application et ses données ne soit pas exposée en frontal sur le web. De plus le SGBD est isolé sur un serveur différent du serveur applicatif
- Chiffrement des données :
  - Méthode AES 128
  - Conservation de la clé de chiffrement dans un environnement sécurisé accessible uniquement localement, scellé par un mot de passe
  - Clé différente entre l'environnement de développement, de production, et de recette.
- Les données échangées via Internet entre la plateforme IBANSecure et les postes Utilisateurs et Administrateurs s'effectuent au travers du protocole sécurisé HTTPS.
- Le protocole utilisé est le standard TLS 1.2 (Transport Layer Security), intégré à la plupart des navigateurs Internet.
- Durée de conservation des données des DDV :
  - Par défaut les données des DDV sont conservées aussi longtemps que la licence qui les a réalisées existe, ceci pour permettre aux utilisateurs de consulter l'historique de toutes les DDV qu'ils ont émises. Les données de la demande et de la réponse sont fusionnées et donc conservées pour la même durée.
  - Les clients qui le souhaitent peuvent paramétrer un délai de conservation des données. Passé ce délai, les données des DDV seront rendues anonymes mais les DDV seront toujours présentes dans l'historique du Client, notamment pour permettre de visionner des statistiques sur les IBAN vérifiés.
  - Si une licence est supprimée, par exemple suite à une demande de résiliation, ses données sont conservées pour 30 jours afin de pouvoir annuler la suppression si nécessaire.

GESTION DES HABILITATIONS

- Restriction de l'accès aux données à caractère personnel et communication des données à caractère personnel uniquement aux personnes ayant besoin d'en connaître, en veillant à ce que ces personnes soient soumises à une obligation contractuelle ou légale de confidentialité et de sécurité appropriée (par écrit et individuellement).
- Chaque collaborateur se voit communiquer le juste niveau d'information et de droits d'accès en fonction des tâches qui lui sont attribuées (principe de moindre privilège)
- Il n'y a pas de comptes génériques, ils sont tous personnalisés et nominatifs.
- La procédure de revue des identifiants et accréditations est systématique et réalisée trimestriellement. Les identifiants inutilisés et les niveaux d'accréditation sont revus, les besoins des accédants sont confirmés. Cette revue est trimestrielle.

JOURNALISATION ET CONTROLES ASSOCIES

- Les accès à la plateforme IBANSecure et actions effectuées sont systématiquement enregistrées de manière sécurisée
- Cet historique est régulièrement consulté afin de déceler des activités potentiellement suspectes.

SECURITE DES DEVELOPPEMENTS

- L'environnement de développement est totalement décorrélé des environnements de recette et de production
- Aucune donnée sensible n'est requise lors des développements, puisque les utilisateurs d'IBANSecure renseignent eux-mêmes les données nécessaires.
- Les éléments chiffrements de production diffèrent de ceux de développement.
- La mise en place des secrets de chiffrement de production ne se fait qu'à la mise en production initiale et lors d'un éventuel renouvellement.
- Les développements informatiques sont réalisés en respectant les standards en matière de sécurité maintenus à jour par une veille constante.
- Chaque inclusion de données personnelles est impérativement chiffrée.

- Le contrôle de l'étanchéité entre licences clients est une règle vérifiée à chaque étape.
- Les failles particulières suivantes font l'objet d'un contrôle constant :
    i. Injection de commande (Ex : SQL)
    ii. Perte d'authentification partielle
    iii. XSS
    iv. Exposition de données personnelles
    v. Contrôle des versions des composants utilisés
    vi. Accès des APIs
- Les développements sont soumis à une validation continue et automatisée. Les règles de cette validation sont définies par l'équipe en charge des développements.
- Une défaillance d'un point de cette chaine entraine une alerte immédiate et un blocage de toute mise en production.
- Le contrôle des vulnérabilités connues se fait grâce à différents outils comme SSLLabs ou Imirhil lors des développements et avant mise en production.

SECURITE PHYSIQUE

- ISILIS identifie et veille à protéger les zones physiques sensibles telles que les centres de traitement (datacenter) et les locaux techniques de ses différents sites
- Pour ce faire, ISILIS s'assure que :
    i. L'accès aux zones physiques sensibles identifiées est sécurisé par l'utilisation de badges électroniques dont l'usage est tracé afin de prévenir un accès non autorisé aux ressources matérielles des systèmes d'information
    ii. Les accès aux zones physiques sensibles sont impossibles au public. Aucune communication ne devra être faite vers l'extérieur sur des données permettant de localiser les emplacements des moyens de traitement.
    iii. Les points d'accès par lesquels des personnes peuvent pénétrer dans les locaux d'ISILIS sont contrôlés
    iv. Les locaux d'ISILIS sont sécurisés

POLITIQUE DE SAUVEGARDE

- Pilotés depuis un réseau d'administration, les données de la plateforme sont sauvegardées sur l'infrastructure de sauvegarde de l'hébergeur.
- Le dispositif de backup permet une sauvegarde complète des machines virtuelles.
- Sauvegarde incrémentale quotidienne, avec une durée de rétention de 7 jours
- Les sauvegardes sont des sauvegardes sur disques hébergées sur le site local de l'architecture active
- Une réplication quotidienne du dernier jeu de sauvegarde est effectuée sur le site de secours (différent du site nominal)

DIVERS

- Les accès à distance sont assurés par VPN à double facteur d'authentification (ID + token), pour des besoins de MCO ou d'administration de la plateforme
- Des réunions de sensibilisation impliquant l'ensemble des collaborateurs d'ISILIS sont organisées annuellement. Par ailleurs tout nouvel entrant doit signer la Charte informatique ISILIS.
- Utilisation de la solution EDR CrowdStrike
- Règles de filtrage pour les sites web identifiés comme malveillants
- Utilisation de Bitlocker pour le chiffrement du disque dur des postes de travail