

OBJET DU DOCUMENT

Ce document a pour objet de fixer les Conditions Générales de fourniture par SMARTPUSH -

Société par Actions Simplifiée au capital de 4 089,48Euros, située au 1 La Canebière, 13001 - Marseille, immatriculée au RCS de Marseille sous le numéro 837 499 102 - 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 des présentes Conditions Générales par le Client. Conformément à l'article L.441-1 du Code de Commerce, les présentes CGV constituent le socle unique de la relation commerciale entre SMARTPUSH et le Client. Elles s'appliquent sans restriction ni réserve, à toutes les prestations, à l'exclusion de tout document émanant du Client, et notamment ses conditions générales d'achat, sauf accord exprès de SMARTPUSH. SMARTPUSH pourra modifier ses CGV à tout moment. Cette modification prendra effet dans un délai d'un (1) mois après leur communication au 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@smartpush.io

LEXIQUE

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

Banque émettrice : Banque partenaire de SMARTPUSH via laquelle les DDV seront émises sur le réseau SEPAmail DIAMOND.

Client : Entreprise utilisatrice du Logiciel IBANSecure.

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

DOCUMENTS CONTRACTUELS

Pour définir et encadrer au mieux les prestations, les Parties entendent donner valeur contractuelle aux documents suivants, classés par ordre hiérarchique de valeur juridique décroissante :

1. Le présent document ;
2. Les Annexes suivantes :

Annexe 1 : Description du traitement faisant l'objet de la gestion déléguée (sous-traitance)

Annexe 2 : Sécurité et modalités de conservation des Données

Annexe 3 : Liste des sous-traitants

En cas de contradiction entre les dispositions du présent document et celles contenues en Annexes, celles du présent document prévaudront.

Les titres des clauses n'ont qu'une valeur indicative, en cas de contradiction entre ces titres et leur contenu, ce dernier fera foi.

DESCRIPTION DES PRESTATIONS

Dans le cadre des présentes, SMARTPUSH s'engage à mettre à disposition du Client l'outil IBANSecure, accessible via le portail web www.ibansecure.fr ainsi que via l'API dédiée. L'outil 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 SMARTPUSH auprès de SEPAmail.

Pour obtenir un identifiant SEPAmail, le Client devra fournir à SMARTPUSH les informations suivantes :

- Appellation juridique
- Adresse du siège : rue, code postal, ville, pays
- Code activité
- SIREN

Cet identifiant SEPAmail devra être renseigné par le Client dans l'interface de paramétrage d'IBANSecure.

FONCTIONNEMENT

Le processus de fonctionnement d'IBANSecure est le suivant :

1. Le Client communique des coordonnées bancaires qu'il souhaite valider via IBANSecure au travers des canaux suivants : renseignement manuel sur le site internet www.ibansecure.fr ou import d'un fichier Excel. En sus des coordonnées bancaires, le SIREN ou le SIRET ou le numéro de TVA est requis pour des personnes morales et le nom et prénom pour des personnes physiques (la date de naissance étant une donnée optionnelle).
2. IBANSecure vérifie les données auprès des banques adhérentes via le service interbancaire SEPAmail DIAMOND. IBANSecure effectue la transmission des coordonnées bancaires à valider auprès de sa banque partenaire, nommée la banque émettrice. Cette dernière interroge alors la banque de la personne physique ou morale détenant le compte adossé aux coordonnées bancaires à valider.
3. La banque émettrice reçoit la réponse qui est ensuite transmise à IBANSecure. IBANSecure la met ensuite à la disposition du client final sur le site www.ibansecure.fr.

Les délais actuels de traitement varient en fonction de la banque émettrice et/ou la banque teneuse du compte à vérifier. Il peut s'écouler de quelques secondes à 48h entre l'émission d'une DDV et la réception de la réponse.

Ces temps de réponse sont amenés à être réduits par les banques afin d'offrir des réponses en temps réel. Il est expressément précisé que la responsabilité du Prestataire ne pourra pas être engagée en raison des délais de traitement de la banque émettrice et/ou la banque teneuse du compte à vérifier.

La présente description des prestations est susceptible d'évoluer, une description à jour est disponible sur www.ibansecure.com/fonctionnement

MODALITES D'ACCES

L'application est accessible 7 jours sur 7, 24 heures sur 24. Cette disponibilité n'est cependant pas garantie contractuellement et, pour les nécessités de maintenance, elle pourra être réduite temporairement.

GESTION DU MOT DE PASSE

Dès la première connexion, avant d'enregistrer des données, le Client choisit lui-même son nom d'accès et son mot de passe pour accéder à IBANSecure (ci-après désignés les « Identifiants »). IBANSecure ne comporte aucune fonctionnalité permettant de connaître le mot de passe d'un utilisateur. Le Client peut toutefois le retrouver via la fonctionnalité prévue à cet effet.

Le Client est responsable du maintien de la confidentialité des Identifiants et doit informer sans délai SMARTPUSH de toute utilisation non autorisée ou perte de tout Identifiant.

De même, le Client est seul responsable de toutes les activités menées avec les Identifiants.

CONDITIONS TARIFAIRES ET FACTURATION

Après acceptation des CGU et complétions des informations de facturation, SMARTPUSH ouvrira la licence d'utilisation du Client lui permettant d'accéder à l'outil.

Le Client souscrit un forfait de vérification valable 12 mois et automatiquement renouvelable, soit lorsque le nombre de DDV défini dans le forfait annuel a été consommé, soit à échéance des 12 mois.

Lorsque le forfait expire, un nouveau forfait est automatiquement généré selon les mêmes termes que le précédent pour assurer la continuité du service, et ce jusqu'à résiliation des présentes.

Une facture sera émise à la création du forfait puis à chaque renouvellement.

A l'issue de la durée de validité du forfait, les DDV qui n'auraient pas été consommées ne pourront ni être re-créditées, ni donner droit à un remboursement.

Le Client choisit le volume de DDV de son forfait, selon les conditions tarifaires standards :

Vérifications/an	Prix unitaire (HT)	Prix du forfait (HT)
500	1,20 €	600 €
1 000	0,90 €	900 €
10 000	0,80 €	8 000 €
50 000	0,70 €	35 000 €
100 000	0,65 €	65 000 €

Ce forfait pourra éventuellement être modifié selon les conditions définies ci-dessous.

MODIFICATION DU FORFAIT ANNUEL

Il est possible de modifier le volume de DDV du forfait en envoyant un mail à SMARTPUSH à l'adresse ibansecure@smartpush.io

Cette demande sera soumise à acceptation de SMARTPUSH. En cas de refus par SMARTPUSH de la demande de révision de la licence, la licence du Client conservera les modalités de la licence en cours (notamment concernant le volume de vérification et le tarif du forfait).

En cas d'acceptation par SMARTPUSH de la demande de modification de la licence :

- Pour une demande portant sur un volume supérieur de DDV annuelles (par rapport au forfait en cours) :
 - La modification aura lieu au choix, sur le forfait en cours ou sur le prochain forfait qui sera renouvelé.
 - Le tarif du forfait en cours ou du prochain forfait sera revu en fonction, selon les conditions tarifaires standards.
 - S'il s'agit d'une augmentation du nombre de DDV du forfait en cours, une facture supplémentaire sera émise au moment du crédit de ces DDV supplémentaires.
- Pour une demande portant sur un volume inférieur de DDV annuelles (par rapport au forfait en cours) :
 - La modification aura lieu sur le prochain forfait qui sera renouvelé.
 - La notification du Client devra intervenir au plus tard deux (2) mois avant la date d'expiration du forfait, ou avant l'épuisement total des demandes de vérification contenues dans le forfait.

DELAÏ DE PAIEMENT

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.

Les factures seront considérées comme acceptées après un délai de dix (10) jours suivant leur réception. En cas de contestation sur une facture, le Client devra, dans ce délai, informer SMARTPUSH par LRAR de réception de la partie contestée et des raisons de la contestation. En tout état de cause, le Client ne pourra retenir que la part des sommes préalablement et dûment contestées.

Le paiement à bonne date constitue un engagement essentiel du Client.

SMARTPUSH se réserve le droit de bloquer l'accès à IBANSecure au Client si le montant de la licence n'est pas réglé dans son intégralité. Dans le cas où le Client n'effectuerait pas le paiement dans les délais convenus, SMARTPUSH 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. Il est convenu que le paiement de pénalités de retard ne pourra pas être exigé sur la part des factures totalement ou partiellement contestées par le Client dans les modalités énoncées ci-dessus. SMARTPUSH pourra également suspendre les prestations, sauf dans l'hypothèse où le Client aurait totalement ou partiellement contesté le montant des factures selon les modalités ci-dessus. En cas de suspension pour ce motif et dans ces conditions, le Client ne pourra se prévaloir d'aucun préjudice du fait de cette suspension.

ASSISTANCE

L'assistance à l'utilisation d'IBANSecure peut être obtenue par e-mail ou par le bouton d'aide présent sur chacune des pages du site tous les Jours Ouvrés de 09H00 à 12H et de 14H00 à 17H. E-mail de contact : ibansecure@smartpush.io

L'assistance est assurée par des techniciens de SMARTPUSH, elle consiste à expliquer le fonctionnement des commandes d'IBANSecure. Les techniciens d'assistance n'ont pas de compétences comptables ni financières, et ils ne connaissent pas les règles de gestion ni organisationnelles du Client. Quelles que soient les indications fournies par les techniciens, le Client est le seul à pouvoir juger des conséquences sur sa propre gestion des choix d'utilisation qu'il peut faire, et il reste seul responsable de ces choix.

OBLIGATIONS DE SMARTPUSH

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

- La disponibilité de ses données et des fonctionnalités de l'application, 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 présentes 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.

OBLIGATIONS DU CLIENT

Le Client s'engage, à titre d'obligation essentielle, à payer à bonne date à SMARTPUSH les sommes dues en contre partie de la réalisation des prestations par SMARTPUSH, conformément aux modalités financières prévues aux présentes. Pour permettre à SMARTPUSH de mener à bien les prestations, le Client s'engage à exprimer de la manière la plus claire possible et la plus exhaustive possible ses besoins. Il s'engage à transmettre à SMARTPUSH dans un délai suffisant les informations nécessaires à la bonne exécution des prestations mises à sa charge.

Par ailleurs, le Client s'engage à mettre à disposition de SMARTPUSH les moyens qui lui sont nécessaires à l'exécution des Prestations. Il lui communiquera notamment, sous un format exploitable aisément par SMARTPUSH, les documents ou informations nécessaires à la réalisation des prestations dans des délais raisonnables, et répondra à toute explication ou demande d'information complémentaire que SMARTPUSH pourra solliciter. Plus généralement, le Client s'engage à mettre au service de SMARTPUSH 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 SMARTPUSH, le cas échéant, de tout évènement ou modification susceptible d'avoir un impact sur la réalisation des prestations.

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

CONDITIONS D'UTILISATION DU SERVICE SEPAMail DIAMOND

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. Enfin, 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 demande à des tiers.

PROPRIETE INTELLECTUELLE

SMARTPUSH 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). SMARTPUSH 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 déchiffrement ou la modification du code source.

RESPONSABILITE

SMARTPUSH 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.

Par ailleurs, la responsabilité de SMARTPUSH 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 de SMARTPUSH 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 CGV ainsi que les instructions du Client. De même, la responsabilité de SMARTPUSH 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 SMARTPUSH des données, dans l'utilisation de ses logiciels, ou encore dans le non-respect des conseils donnés par SMARTPUSH. Le Client reconnaît 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. SMARTPUSH décline 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 SMARTPUSH 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 de SMARTPUSH ne pourra être engagée pour un montant excédant un (1) mois moyen de facturation (sur la base des 12 derniers mois). Il est entendu que SMARTPUSH 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, SMARTPUSH 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 ;

SMARTPUSH – CONDITIONS GENERALES D'UTILISATION D'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 CGV et ce pour quelque cause que ce soit.

FORCE MAJEURE

La survenance d'un cas de force majeure emportera suspension des obligations nées des CGV, 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 des Parties ne pourra donc 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 événements suivants : les grèves et conflits sociaux internes ou externes à l'entreprise, les épidémies, l'impossibilité d'approvisionnement pour quelque raison que ce soit, les catastrophes naturelles et les événements climatiques exceptionnels, les épidémies et pandémies, 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. La Partie qui invoquera un cas de force majeure devra, dès la survenance de celui-ci, en aviser l'autre Partie par tout moyen. Les faits devront être confirmés dans les meilleurs délais par lettre recommandée avec avis de réception, indiquant la nature et les caractéristiques des faits. La Partie empêchée prendra sans délai toute mesure appropriée en vue de remédier à cette situation, et en tout état de cause de tenter d'en limiter les effets. Les Parties conviennent de se réunir dans les plus brefs délais afin d'examiner les conditions commerciales, opérationnelles et financières pouvant permettre la poursuite de l'exécution des prestations.

Si le cas de force majeure devait durer plus de 30 jours consécutifs, entraînant une diminution voire une suspension de l'exécution des prestations, ces dernières pourront être résiliées par l'envoi d'un courrier recommandé avec avis de réception dans les conditions prévues dans ce courrier et sur lesquelles les Parties se seront préalablement entendues.

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 présentes 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 SMARTPUSH 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.

SMARTPUSH 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, SMARTPUSH 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 SMARTPSUH.

DONNEES SIGNALÉTIQUES

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.

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 réglementation 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 Réglementation).

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

CARACTERISTIQUES DU TRAITEMENT

Les caractéristiques des traitements de données à caractère personnel effectués par le sous-traitant 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. Toute modification de l'annexe n° 1 devra donner lieu à l'établissement d'un avenant signé par les Parties.

OBLIGATIONS DU SOUS-TRAITANT**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 que SMARTPUSH n'y soit tenu d'y procéder en vertu du droit applicable.
Dans ce cas, SMARTPUSH 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 en vertu des présentes 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; (Eric Frichot– dpo@smartpush.io)
- 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, 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.

Sécurité, confidentialité, violation et destruction des données

Le sous-traitant s'engage à :

- Mettre en œuvre les mesures de sécurité décrites en Annexe des présentes 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 prestations et détruire les copies existantes, ainsi que lui communiquer la preuve de ces destructions.

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@smartpush.io
- Mettre à disposition du Client toutes les informations nécessaires pour démontrer le respect des obligations énoncées aux présentes 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 ULTERIEURE

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 que SMARTPUSH pourra sous-traiter tout ou partie des Prestations à une ou plusieurs sociétés de son groupe, 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.

TRANSFERTS DE DONNEES A CARACTERE PERSONNEL HORS-UE

SMARTPUSH 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 SMARTPUSH 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.

DUREE ET RESILIATION POUR CONVENANCE**ENTREE EN VIGUEUR - DUREE**

Les présentes CGV prennent effet à la date de leur acceptation en ligne pour une durée indéterminée.

RESILIATION POUR CONVENANCE

Les présentes CGV pourront être résiliées à tout moment par l'une ou l'autre des Parties en respectant un délai de préavis de trois (3) mois, et ce après envoi d'une lettre recommandée avec avis de réception de signification de résiliation.

Dans le cas où le renouvellement du Forfait annuel interviendrait pendant le délai de préavis, ledit forfait sera renouvelé et valable uniquement jusqu'à la fin du préavis. Le Client sera redevable des factures associées. Tous les droits d'utilisation et d'exploitation des attributs de propriété intellectuelle consentis au titre des présentes prendront fin à la date de cessation des prestations pour quelque cause que ce soit.

Conséquences de la résiliation pour convenance pour le Forfait annuel et le Mode Batch :

La résiliation des CGV ne pourra en aucun cas donner droit à un remboursement.

RESILIATION POUR MANQUEMENT

Les présentes pourront être résiliées à tout moment en cas d'inexécution par une Partie de l'une de ses obligations essentielles ayant des conséquences graves pour l'autre Partie. Dans ce cas, un comité de pilotage exceptionnel se réunira sur convocation de la Partie la plus diligente et ce afin de mettre en place un plan d'actions conjoint visant à la résolution des problématiques rencontrées. A défaut d'effet de ce plan dans un délai de 15 jours ouvrés à compter de sa mise en place, les dirigeants de chacune des Parties se rencontreront sur convocation de la Partie diligente et dans un délai maximal de huit (8) jours ouvrés à compter du constat d'échec du plan d'actions et ce afin de décider des suites à donner aux présentes. En cas de désaccord de ces derniers, les présentes seront résiliées 30 jours après l'envoi d'un courrier recommandé avec avis de réception par l'une ou l'autre des Parties et faisant état de la volonté de celle-ci de mettre un terme aux prestations. Cette résiliation interviendra sans préjudice des indemnités que la Partie lésée sera éventuellement susceptible de réclamer en réparation de son préjudice, dans les limites éventuellement définies aux présentes. Pendant la période de préavis, les relations entre SMARTPUSH et le Client se poursuivront de façon normale, loyale et sincère, chacune des Parties s'engageant à respecter scrupuleusement ses obligations telles que découlant des présentes. En cas de résiliation des présentes, pour quelque cause que ce soit, SMARTPUSH s'engage, selon le choix du Client, et sous réserve du complet paiement des prestations effectuées à :

- Restituer à première demande du Client les consommables non encore utilisés,
- Ou terminer les prestations en cours.

SMARTPUSH s'oblige par ailleurs à retourner à première demande du Client les fichiers qui lui ont été transmis.

COMMUNICATION

Chaque Partie reconnaît et accepte que l'autre Partie puisse utiliser le nom de l'autre Partie à titre de référence commerciale. Les Parties pourront effectuer des opérations de communication externe par tout moyen (audiovisuel, voie de presse ou autre) relative à leur partenariat, sous réserve d'obtenir l'accord exprès de l'autre Partie sur ladite opération avant toute diffusion.

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 (SOUS-TRAITANCE)

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 des présentes CGV, 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
Expert technique indépendant	Tierce Maintenance Applicative	41100 Vendôme, France
SAFE0	Hébergement	Datacenter Equinix PA6 10 rue Waldeck Rochet 520 93300 Aubervilliers, France

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, notamment le datacenter PA6 localisé à Aubervilliers, qui dispose 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 pour une durée de un (1) an, pour permettre aux utilisateurs de consulter l'historique de toutes les DDV qu'ils ont émises. Les données utilisées pour la requête et celles de la réponse sont fusionnées et donc conservées pour la même durée.
 - Les clients qui le souhaitent peuvent paramétrer un délai de conservation plus court.
 - Passé ce délai, les données personnelles des DDV seront effacées mais les résultats des DDV seront toujours présents dans l'historique du Client (retour positif, négatif, ou autre et date de vérification), ceci pour des raisons de maintenance applicative et d'amélioration continue, et pour permettre la réalisation de statistiques sur l'utilisation de la solution.
 - 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.

SMARTPUSH – CONDITIONS GENERALES D'UTILISATION D'IBANSECURE

- 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 chaîne entraîne une alerte immédiate et un blocage de toute mise en production.
- Le contrôle des vulnérabilités connues se fait grâce à différents outils comme SSL Labs ou Imirhil lors des développements et avant mise en production.

SECURITE PHYSIQUE

- SMARTPUSH 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, SMARTPUSH 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 de SMARTPUSH sont contrôlés
 - iv. Les locaux de SMARTPUSH 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 de SMARTPUSH sont organisées annuellement. Par ailleurs tout nouvel entrant doit signer la Charte informatique SMARTPUSH.
- 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

ANNEXE 3: Liste des destinataires de données a caractère personnel

Service Sepamail Diamond Société Générale, 29 Bd Haussmann, 75009 Paris.