

Contrat de Sous-traitance Traitement de Données Personnelles

[**SOCIÉTÉ DU CLIENT**], situé à [**VILLE DU CLIENT**] et représenté par [**NOM DU CLIENT**] *

(ci-après, « *le responsable de traitement* »)

d'une part,

ET

IABAKO, société par actions simplifiée au capital de 15 000€, RCS 834 576 522 Paris, situé à 78 Avenue des Champs Elysées, 75008, Paris, France (ci-après, « *le sous-traitant* »)

d'autre part,

* Un contrat de sous-traitance sur le traitement des données personnelles sera mis à disposition pour chaque client. Les informations du responsable de traitement seront remplacées par les informations nominatives du client. Le responsable du traitement pourra télécharger le contrat sur son compte.

I. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après, « *le règlement européen sur la protection des données* »).

II. Description du traitement faisant l'objet de la sous-traitance

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir les services de facturation et gestion en ligne.

La nature des opérations réalisées sur les données est : collecte et conservation et des données personnelles.

- Collecte : Le Responsable de traitement, est le seul à décider de la nature, du but et de l'utilisation des informations personnelles saisies que ce soit des informations générales (nom, prénom, date de naissance), de contact (adresse, téléphone), ou bien plus spécifiques (champs personnalisés de clients).
- Conservation : le stockage des données saisies est réalisé par le sous-traitant sur des serveurs sécurisés localisés en France (cf chapitre V).

La ou les finalités du traitement sont :

- Gestion de devis, gestion de factures, gestion de bons de commande, relance d'impayés, envoi des messages client, suivi des échanges client (actions à faire, suivi des RDV).
- Gestion de commandes d'achat fournisseurs
- Suivi de Livraisons
- Service client

Les données à caractère personnel traitées sont :

- Sexe
- Nom
- Pré nom
- Date de naissance
- Téléphone(s)
- Adresse(s)
- Code postale
- Pays
- e-mail
- Coordonnées Bancaires

Les catégories de personnes concernées sont :

Clients, prospects, fournisseurs.

Le Responsable de traitement peut, à tout moment, accéder à son compte pour pour gérer ses données : consulter, modifier, extraire, supprimer toute l'information. Egalement, le Responsable du traitement peut, à tout moment, fermer son compte. Il peut adresser la clôture de son compte y compris la suppression des données, en envoyant un mail à @dpo@iabako.com.

III. Accord du contrat

Afin de pouvoir utiliser les services proposés par le sous-traitant, le responsable de traitement doit accepter les conditions d'utilisation, la politique de confidentialité ainsi que le présent contrat de sous-traitance de traitement des données personnelles. Le cas échéant, le responsable de traitement ne pourra pas utiliser lesdits services.

Le responsable du traitement donne son accord sur le présent contrat de sous-traitance de traitement des données personnelles en acceptant les conditions d'utilisation et la politique de confidentialité (protection de données), lors du processus d'inscription au service en ligne proposé par le sous-traitant.

IV. Durée du contrat

Le présent contrat entre en vigueur à compter de l'inscription du responsable de traitement au service en ligne proposé par le sous-traitant, suite à son accord

sur les conditions d'utilisation, la politique de confidentialité (protection de données) et le présent contrat de sous-traitance.

La durée du contrat est déterminée par la date de fin des abonnements souscrits (mensuels, annuels, essai gratuit) ; date à laquelle la relation Responsable du traitement et sous-traitant prendra fin.

Egalement, le contrat prendra fin lorsque le Responsable du traitement décide de fermer son compte. Le Responsable de traitement peut arrêter l'utilisation du service en clôturant son compte. Une demande de fermeture de compte (y compris la suppression de l'information) peut être envoyée par mail à tout moment à dpo@iabako.com.

V. Obligations du sous-traitant vis-à-vis du responsable de traitement

Le sous-traitant s'engage à :

1. traiter les données *uniquement pour les seules finalités* qui font l'objet de la sous-traitance
2. *garantir la confidentialité* des données à caractère personnel traitées dans le cadre du présent contrat
3. veiller à ce que les *personnes autorisées à traiter les données à caractère personnel* en vertu du présent contrat :
 - s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité
 - reçoivent la formation nécessaire en matière de protection des données à caractère personnel
5. 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*

6.Sous-traitance :

Le sous-traitant peut faire appel à un autre sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Le responsable de traitement dispose d'un délai minimum de 1 mois à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations.

7.Droit d'information des personnes concernées

Il appartient au responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

8.Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification,

d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique à dpo@iabako.com.

9. Notification des violations de données à caractère personnel

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans un délai maximum de 72 heures après en avoir pris connaissance et par email. Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Après accord du responsable de traitement, le sous-traitant notifie à l'autorité de contrôle compétente (la CNIL), au nom et pour le compte du responsable de traitement, les violations de données à caractère personnel dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

La notification contient au moins :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;

- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

Après accord du responsable de traitement, le sous-traitant communique, au nom et pour le compte du responsable de traitement, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à

caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

10. Aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations

Le sous-traitant aide le responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données.

Le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

11. Mesures de sécurité

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité suivantes :

Accès sécurisé et confidentialité

La navigation sur le site du sous-traitant est privée et protégée grâce aux technologies SSL (https). Aucune autre personne à part le Responsable de traitement (ou toute autre personne désignée par le Responsable de traitement) n'aura accès à ces informations saisies.

Mot de passe : Seul le Responsable du traitement a accès à ses données. L'utilisation d'un mot de passe confidentiel et sécurisé est obligatoire (au moins huit caractères, lettres et chiffres). Il est stocké chiffré dans les bases de données du sous-traitant, par une fonction (de type hash) irréversible. Le sous-traitant ne connaît pas le mot de passe et donc n'est pas en mesure de le communiquer. En cas d'oubli, le Responsable du traitement doit choisir un nouveau mot de passe, après vérification d'un code de sécurité envoyé par courrier électronique.

Il est interdit de partager les informations de connexion à de tiers. Le sous-traitant met à disposition des accès sécurisés pour des tiers autorisés (i.e comptable, équipe).

Traçabilité

Habilitations : le sous-traitant fournit, à la demande, des accès sécurisés pour des utilisateurs supplémentaires, désignés par le Responsable du traitement. Ces accès sont entièrement gérés par le Responsable du traitement, tels que : des habilitations au niveau des droits (suppression, consultation, modification) et de type d'accès (par module et type d'information), et ce, pour chaque utilisateur. Cette option est gérée dans le menu « Utilisateurs ».

Activité : le sous-traitant met à disposition un suivi d'activité journalière des actions menées dans l'outil (modification, suppression, ajout des données), et ce, pour chaque utilisateur. Ce suivi est disponible dans la page principale « Suivi d'activité ».

Conservation des données :

Toutes les données saisies sont stockées dans des serveurs hautement sécurisés. Egalement, des copies journalières de sécurité sont réalisées sur deux serveurs distincts pour diminuer au maximum le risque de perte des données. Cf [politique de confidentialité de AWS](#).

Protection du logiciel :

En outre, le sous-traitant réalise de tests de sécurité, des correctifs et des mises à jour régulières afin de garantir le bon fonctionnement du service.

En cas de panne du système, le sous-traitant s'engage à rétablir le système sous 48h.

12.Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, et après le temps réglementaire (six ans) de conservation de données relatives aux transactions de facturation et paiement réalisées par le responsable de traitement, le sous-traitant s'engage à détruire toutes les données à caractère personnel.

13. Délégué à la protection des données

Le sous-traitant doit communiquer au responsable de traitement, suite à une demande écrite de la part du responsable de traitement, *le nom et les coordonnées de son délégué à la protection des données.*

14. Registre des catégories d'activités de traitement

Le sous-traitant déclare *tenir par écrit un registre* de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement.

Le responsable de traitement peut demander le registre des activités de traitement pour consultation à l'adresse dpo@iabako.com.

Ce registre doit contenir le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;

- les catégories de traitements effectués pour le compte du responsable du traitement ;
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins : le chiffrement des données à caractère personnel, des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement; des moyens permettant de rétablir la disponibilité des données à caractère

personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique; une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

15.Documentation

Le sous-traitant met à la disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

VI. Obligations du responsable de traitement vis-à-vis du sous-traitant

Le responsable de traitement s'engage à :

1. accepter et respecter les conditions d'utilisation, la politique de confidentialité et le présent contrat de sous-traitance de traitement des données personnelles.
- 2.fournir au sous-traitant les données visées au II des présentes clauses.
- 3.veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du sous-traitant.
- 4.superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant.