DATA PROCESSING AGREEMENT

(Version du 25 septembre 2019)

Le présent Data Processing Agreement définit les principes et engagements applicables au Traitement de données à caractère personnel principal. Les Parties conviennent que pour une certaine partie des traitements, les parties peuvent avoir un rôle différent et être alternativement soit responsable de traitement, soit sous-traitant, soit responsable conjoint du traitement. Les obligations afférentes à ces cas particuliers sont régies par l'Annexe A.

Préambule

Le présent Data Protection Agreement (ci-après le **« DPA »**) fait partie intégrante de tout accord écrit entre Odiso (ci-après « **Odiso** » ou le « **Prestataire** ») et le Client, en ce compris des Conditions Générales de Services de Odiso, du ou des bons de commande et/ou facture(s) ayant pour objet l'achat d'une prestation de service fournie par Odiso (ci-après le **« Contrat »**).

En fonction de la chaîne contractuelle, le Client peut être responsable du traitement, responsable conjoint du traitement vis-à-vis d'un tiers ou lui-même un sous-traitant d'un responsable de traitement (ci-après le **« Client Final »**).

En tout état de cause, le Prestataire ne s'engage, en tant que sous-traitant, qu'auprès du Client dans le cadre des présentes.

Le Client, même sous-traitant du Client Final, a les prérogatives et obligations de ce dernier vis-à-vis du Prestataire. A cet effet, le Client demeure seul responsable vis-à-vis du Client Final et devra notamment s'assurer (i) que toutes instructions qu'il pourrait donner au Prestataire sont émises sur la base d'instructions documentées du Client Final ; (ii) que le Client Final a autorisé le Client à faire appel au Prestataire en tant que sous-traitant conformément au contrat qui les lie ; et (iii) que le contrat le liant au Client final prévoit des obligations équivalentes à celles prévues dans les présentes.

Il est entendu entre les Parties que le présent DPA annule et remplace toutes dispositions concernant les exigences de la règlementation applicable relative à la Protection des Données à caractère personnel présentes au sein du Contrat et que les clauses du présent DPA prévalent en conséquence sur celles dudit Contrat.

I - Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles (i) le Prestataire s'engage à effectuer pour le compte du Client les opérations de traitement de données à caractère personnel définies ci-après (ii) le Client donne ses instructions au Prestataire pour tous les traitements de données à caractère personnel.

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 RGPD**»).

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

A. Nature et finalité du traitement

Le Prestataire est autorisé à traiter pour le compte du Client les données à caractère personnel nécessaires pour fournir le ou les service(s) d'hébergement tel(s) que décrit(s) dans le ou les Contrat(s).

La finalité du traitement est strictement limitée au service d'hébergement tel que détaillé dans le Contrat, à l'exception de toute autre finalité. A ce titre, le Prestataire s'engage expressément (i) à ne pas accéder et/ou utiliser lesdites données sauf si cela est strictement nécessaire pour fournir ledit service d'hébergement et (ii) à ne pas utiliser ou traiter lesdites données pour ses propres besoins et notamment à ne pas utiliser ou traiter lesdites données à des fins de profilage, de data mining ou de marketing direct.

B. Catégories de données personnelles concernées

Afin d'effectuer sa prestation d'hébergement conformément à la demande du Client (et uniquement à cette fin) le Prestataire pourra être amené à traiter les catégories de données personnelles suivantes :

Les informations personnelles de contact : noms, prénoms, adresse postale, numéro de téléphone fixe et mobile, numéro de fax, adresse email ; **les informations relatives à la situation familiale, au mode de vie et à la situation sociale** incluant l'âge, le genre, la date de naissance, le statut marital, la composition du foyer, les noms et prénoms des conjoints et enfants ; **des informations relatives à l'emploi** : performance au travail et autres compétences, intitulé du poste et fonction, nom du service, années d'ancienneté, antécédents professionnels, salaires et primes, diplômes, numéro d'identification, informations relatives à la sécurité sociale et coordonnées relatives au lieu de travail ; des **informations financières** ; **bien et services fournis** ; **Identifiant unique collecté depuis des appareils mobiles, adresses IP et données comportementales en ligne**.

C. Catégories de personnes concernées

Les catégories de personnes dont les données personnelles sont susceptibles d'être traitées dans le cadre de la prestation d'hébergement peuvent inclure notamment : vos utilisateurs finaux des produits et/ou services, vos clients, prospects, candidats, employés, fournisseurs, prestataires externes, sous-traitants et contractants.

D. Catégories supplémentaires de données personnelles et de personnes concernées supplémentaires / Données sensibles

En tant qu'hébergeur fournissant une solution Iaas (Infrastructure as a Service), le Prestataire se contente de mettre à disposition du Client un espace de stockage accessible en ligne de manière sécurisé et une infrastructure informatique. Ainsi, un Client utilisant le service d'Hébergement a la liberté de choisir quelles données il souhaite traiter sur l'infrastructure mise à sa disposition, dans quels pays, à quelles fins et comment il souhaite protéger ces données. Compte tenu de la nature du service qu'il délivre, le Prestataire n'a pas à savoir quelles sont les données traitées par le Client et par conséquent, ne peut pas distinguer s'il s'agit de données à caractère personnel ou non. A cette fin, Odiso s'engage à fournir un niveau de sécurité adapté à tout type de données, à l'exception de certaines données sensibles.

En conséquence, toutes les autres catégories de données ou de personnes concernées que celles décrites ci-dessus devront spécifiquement être communiquées au Prestataire par le Client. Le Client s'engage à ne pas héberger de données sensibles au sens de la réglementation en vigueur sans en avoir préalablement averti le Prestataire. En tout état de cause, le Client s'engage à ne pas héberger de données nécessitant la mise en place de mesures de sécurité spécifiques et particulières, autres que celles implémentées par le Prestataire et figurant sur le site internet accessible à l'adresse https://www.odiso.com/mentions-legales.

III - Durée Data Processing Agreement

Si la date de conclusion du Contrat est **antérieure** à la date 25 mai 2018, le présent DPA entre en vigueur à compter du 25 mai 2018 pour la durée stipulée au sein dudit Contrat.

Si la date de conclusion du Contrat est **postérieure** à la date du 25 mai 2018, le présent DPA entre en vigueur à compter de la date de prise d'effets du Contrat et pour la durée stipulée au sein dudit Contrat.

IV - Obligations du Prestataire vis-à-vis du Client

Le Prestataire s'engage à :

1. traiter les données **uniquement pour la ou les seule(s) finalité(s)** qui fait/font l'objet de la sous-traitance.
2. traiter les données **conformément aux instructions** du Client. A cette fin, le Prestataire met à disposition du Client **les fonctionnalités nécessaires lui permettant d'instruire le traitement** par l'utilisation même du service. En effet, le Prestataire met à la disposition du Client une infrastructure virtuelle à la demande et autogérée. Ladite infrastructure lui permet notamment de télécharger des données personnelles, et le cas échéant, déterminer la façon dont ces données personnelles sont traitées. Pour toute instruction complémentaire, le Client peut à tout moment transmettre au Prestataire toute instruction documentée qu'il jugerait nécessaire via l'outil de ticketing ou à l'adresse mail suivante : serviceclient@odiso.com.

   Si le Prestataire considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de

l'Union ou du droit des Etats membres relative à la protection des données, il en **informe dans les meilleurs délais** le Client. En outre, si le Prestataire est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, il doit informer le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

3. garantir la **confidentialité** des données à caractère personnel traitées dans le cadre du présent Data Processing Agreement
4. veiller à ce que les **personnes autorisées à traiter les données à caractère personnel** en vertu du présent Data Processing Agreement:
    a. s'engagent à respecter la **confidentialité** ou soient soumises à une obligation légale appropriée de confidentialité
    b. 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 conception** et de **protection des données par défaut**.

6. Sous-traitance

Le Client autorise expressément le Prestataire à faire appel à des sous-traitants ultérieurs pour mener des activités de traitements prévues au Contrat.

La liste des sous-traitants ultérieurs du Prestataire est disponible à la page suivante : https://www.odiso.com/mentions-legales.

Le Prestataire s'engage à informer préalablement le Client par email en cas de changement concernant l'ajout ou le remplacement de Sous-traitants ultérieurs afin de permettre au Client d'émettre des objections à ces changements.

Toute objection devra être dument justifiée et adressée par le Client dans les meilleurs délais. Le défaut de réponse du Client dans un délai de dix (10) jours ouvrés à compter de l'information par le Prestataire vaut accord du Client au changement.

Si le Client s'oppose à l'ajout d'un nouveau sous-traitant ultérieur par Odiso et que l'exécution du Contrat ne peut pas être poursuivie sans avoir recours au sous-traitant ultérieur concerné, Odiso et le Client pourront dans ce cadre résilier :

- Le Contrat, à condition que le ledit Contrat ne puisse être poursuivi dans sa totalité qu'en ayant recours au sous-traitant ultérieur concerné ; ou
- La partie du Contrat relative au service qui ne peut être raisonnablement fournie sans avoir recours au nouveau sous-traitant ultérieur contesté.

Le Contrat pourra être résilié par lettre recommandée avec avis de réception moyennant le respect d'un préavis de trente (30) jours à compter de l'envoi de ladite lettre, le cachet de la

poste faisant foi. A ce titre, les sommes dues pour les prestations déjà réalisées ne peuvent être contestées par le Client.

Le Prestataire s'engage à conclure un acte juridique avec le sous-traitant ultérieur et à imposer les mêmes obligations que celles applicables au Prestataire vis-à-vis du Client au titre du présent DPA. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le Prestataire demeure pleinement responsable devant le Client de l'exécution par l'autre Prestataire de ses obligations.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent DPA pour le compte et selon les instructions du Client. Il appartient au Prestataire 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 Prestataire demeure pleinement responsable devant le Client de l'exécution par l'autre sous-traitant de ses obligations.

7. Droit d'information des personnes concernées

Il appartient au Client 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 Prestataire doit aider le Client 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).

9. Notification des violations de données à caractère personnel

Le Prestataire notifie au Client toute violation de données à caractère personnel dans le délai légal en vigueur après en avoir pris connaissance, par courrier électronique avec accusé réception. Cette notification est accompagnée de toute documentation utile afin de permettre au Client, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Cette documentation 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 Prestataire 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.

10. Aide du Prestataire dans le cadre du respect par le Client de ses obligations

Le Prestataire aide le Client pour la réalisation d'analyses d'impact relative à la protection des données. Le Prestataire aide le Client pour la réalisation de la consultation préalable de l'autorité de contrôle.

11. Mesures de sécurité

Le Prestataire s'engage à mettre en œuvre les mesures de sécurité décrites sur le site web de Odiso à l'adresse suivante : https://www.odiso.com/mentions-legales .

12. Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le Prestataire s'engage, et sans préjudice des modalités décrites dans le Contrat :

- ✓ à renvoyer toutes les données à caractère personnel au client ou
- ✓ à renvoyer les données à caractère personnel au sous-traitant désigné par le Client

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du Prestataire. A la demande du Client et une fois les données détruites, le Prestataire justifiera par écrit, dans un délai raisonnable, de la destruction des données.

13. Délégué à la protection des données

Le Prestataire communique au Client **le nom et les coordonnées de son délégué à la protection des données**, s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données.

14. Registre des catégories d'activités de traitement

Le Prestataire déclare **tenir par écrit un registre** de toutes les catégories d'activités de traitement effectuées pour le compte du Client comprenant :

- ✓ le nom et les coordonnées du Client 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 :
    - la pseudonymisation et 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 Prestataire met à la disposition du Client la **documentation nécessaire pour démontrer le respect de toutes ses obligations.**

16. Audit

Le Client pourra procéder, à ses frais, à un (1) audit des mesures de protection et de sécurité des données à caractère personnel prises par le Prestataire relativement aux données à caractère personnel traitées pour le compte du Client, au maximum une fois tous les douze (12) mois sauf circonstance exceptionnelle tenant à la violation de données à caractère personnel imputable au Prestataire justifiant de la conduite d'un audit additionnel.

Cet audit pourra être effectué par le Client ou un auditeur tiers indépendant du Prestataire dûment mandaté par le Client, pour autant que cet auditeur tiers n'exerce pas également lui-même une activité concurrente de celle du Prestataire et/ou n'ait aucun lien juridique avec un concurrent du Prestataire.

Un accord de confidentialité devra être signé préalablement entre les Parties et le tiers auditeur.

Le Client devra informer, moyennant le respect d'un préavis de quinze (15) jours ouvrés, le Prestataire par écrit de son intention de faire procéder à un tel audit et de l'identité du tiers auditeur retenu le cas échéant (accompagné du mandat confié) ainsi que du périmètre de l'audit envisagé.

L'audit diligenté par le Client portera uniquement sur le respect des obligations du Prestataire aux termes de la règlementation sur la protection des données à caractère personnel en vigueur, notamment en termes de sécurité et de protection des données à caractère personnel traitées pour le compte du Client au titre du Contrat.

En tout état de cause, les opérations d'audit ne devront pas perturber le fonctionnement des services et l'activité du Prestataire.

V. Obligations du Client vis-à-vis du Prestataire

Le Client s'engage à :

1. Documenter par écrit toute instruction concernant le traitement des données par le Prestataire ou à utiliser les fonctionnalités mises à sa disposition pour instruire le traitement conformément à la réglementation en vigueur.
2. 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 Prestataire.
3. Déterminer les finalités et les moyens du traitement conformément à la réglementation en vigueur. A ce titre, il s'engage notamment à respecter les principes de finalité, de minimisation, de limitation de la durée de conservation des données et s'engage à informer les personnes concernées par le traitement en s'assurant notamment du recueil conforme du consentement.
4. Tenir un registre détaillé des traitements qu'il réalise.
5. Mettre en place les mesures techniques et organisationnelles nécessaires au regard de la réglementation en vigueur.
6. Utiliser le(s) services proposé(s) par Odiso conformément à a la réglementation en vigueur.

ANNEXE A – QUALIFICATION ET OBLIGATIONS RELATIVES AU TRAITEMENT SECONDAIRE

Odiso est qualifié de « responsable de traitement » lorsqu'elle détermine les finalités et les moyens de ses propres traitements. Les données que vous hébergez sur Odiso ne sont pas visées.

Ainsi Odiso peut être amené à collecter des données à des fins de facturation, de gestion des recouvrements, de l'amélioration des services et de la performance, de démarchage commercial ou dans le cadre de la gestion des comptes et des mots de passe de ses clients. A ce titre, les données de certains de vos salariés ayant une interaction avec Odiso peuvent être concernées par ledit traitement.

Odiso s'engage à respecter l'ensemble de la réglementation en vigueur sur les traitements pour lesquels il est responsable de traitement au sens du RGPD et notamment à :

- Limiter la collecte de données à celles strictement utiles pour le traitement
- Ne pas utiliser les données collectées à d'autres fins que celles pour lesquelles elles ont été collectées
- Respecter l'ensemble des bases légales relatives à la durée de conservation
- Ne pas transférer des données à des tiers que ceux intervenant dans le cadre de l'exécution du contrat
- Mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un haut niveau de sécurité