

ACCORD DE PROTECTION ET DE CONFIDENTIALITE DES DONNEES DATA PROCESSING AGREEMENT

Dernière mise à jour : 13 mai 2022

Le Data Processing Agreement (ci-après le « DPA ») fait partie intégrante des Conditions Générales de Vente et prévaut sur toute autre disposition échangée entre les Parties sur le même objet. En cas de conflit entre les dispositions des Conditions Générales de Vente et du présent DPA, les dispositions du DPA prévaudront.

Le DPA a ainsi pour objet de définir les conditions dans lesquelles SOCIALSHAKER (identifié ci-après comme le « Sous-traitant ») s'engage à effectuer pour le compte du CLIENT (identifié ci-après comme le « Responsable de traitement ») et selon ses instructions, les opérations de traitement de données personnelles définies aux présentes.

Le Responsable de traitement reconnaît que le Sous-traitant aura accès, dans le cadre des prestations, à des données personnelles (ci-après « les Données Personnelles »).

Le Responsable de traitement autorise le Sous-traitant, pour la durée et les seuls besoins des Conditions Générales de Vente, à procéder au traitement des Données Personnelles.

Le Responsable de traitement demeure seul responsable du traitement des Données Personnelles.

Il est préalablement entendu entre les Parties que les définitions au sein du présent DPA ont le sens qui leur est donné le Règlement Européen 2016/679 relatif à protection des données personnelles (ci-après, le « RGPD »).

1. CARACTÉRISTIQUES DU TRAITEMENT DE DONNÉES PERSONNELLES

1.1 Dans le cadre des prestations, le Sous-traitant est autorisé à traiter pour le compte du Responsable de traitement les Données Personnelles nécessaires pour fournir le ou les prestation(s) mentionnés dans l'Annexe 1 du présent DPA.

1.2 Le Responsable de traitement pourra donner des instructions plus précises par courrier électronique au Sous-traitant sur le type de Données Personnelles à traiter ainsi que sur les catégories de personnes concernées avant la mise en œuvre du traitement.

1.3 En cas de modification des instructions documentées par le Responsable de traitement, ce dernier ou, le cas échéant, son Délégué à la Protection des Données doit les adresser au Sous-traitant, par écrit, au moins trente (30) jours avant que ces instructions soient appliquées au traitement des Données Personnelles. Dans l'hypothèse où la modification des instructions par le Responsable de traitement aurait un impact matériel sur les prestations du Sous-traitant, ce dernier se réserve le droit de refuser lesdites modifications si celles-ci ne sont pas obligatoires pour le respect des dispositions en matière de protection des Données Personnelles ou de majorer les conditions financières pour tenir compte de cet impact matériel.

2. OBLIGATIONS DES PARTIES

2.1 Obligations du Responsable de traitement. Le Responsable de traitement s'engage à :

2.1.1 documenter par écrit toute instruction concernant le traitement des Données Personnelles par le Sous-traitant ;

- 2.1.2 veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le RGPD de la part du Sous-traitant ;
- 2.1.3 superviser le traitement, y compris réaliser les audits et les inspections auprès du Sous-traitant ;
- 2.1.4 mettre en œuvre les mesures techniques et organisationnelles appropriées pour assurer la sécurité des Données Personnelles qui ne relèvent pas du périmètre du Sous-traitant ;
- 2.1.5 respecter le principe de minimisation des Données Personnelles en ne collectant que ce qui est strictement nécessaire à la ou les finalité(s) pour laquelle les Données Personnelles sont traitées ;
- 2.1.6 s'assurer que le traitement repose sur un fondement juridique, et notamment s'assurer qu'il a reçu le consentement des personnes concernées lorsque ce dernier est nécessaire ;
- 2.1.7 fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des Données Personnelles.

Pour l'exécution des Conditions Générales de Vente, le Responsable de traitement met à la disposition du Sous-traitant les coordonnées de son Délégué à la Protection des Données.

2.2 Obligations générales du Sous-traitant.

2.2.1 Dans le cadre de ses prestations et tout au long de la durée des Conditions Générales de Vente, le Sous-traitant s'engage notamment à :

- 2.2.1.1 respecter les consignes du Responsable de traitement et à ne traiter les Données Personnelles que sur instructions du Responsable de traitement et exclusivement pour son compte et non, sauf les cas où il y est expressément autorisé, pour ses besoins propres ou pour le compte de tiers. Si le Sous-traitant constate que des instructions du Responsable de traitement sont en contradiction avec le RGPD ou des dispositions nationales relatives à la protection des données, il en informera immédiatement le Responsable de traitement et pourra refuser l'exécution desdites instructions tant que la conformité au RGPD et aux dispositions nationales relatives à la protection des données ne sera pas assurée sans engager sa responsabilité ni subir aucune pénalité ;
- 2.2.1.2 prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des Données Personnelles dès la conception et de protection des Données Personnelles par défaut ;
- 2.2.1.3 ne prendre aucune copie des Données Personnelles, à l'exception, le cas échéant, de celles nécessaires à l'exécution de ses prestations ;
- 2.2.1.4 ne pas utiliser les Données Personnelles pour des finalités autres que celles spécifiées dans les Conditions Générales de Vente, ou seulement après avoir recueilli l'accord préalable du Responsable de traitement ;
- 2.2.1.5 ne pas effectuer de transfert de données en dehors de l'Espace Economique Européen sans l'autorisation écrite du Responsable de traitement. Si le transfert est autorisé, le Sous-traitant s'engage à mettre en œuvre les garanties appropriées, conformément à l'article 46 du RGPD. En outre, s'il est tenu de procéder à un transfert des Données Personnelles vers un pays tiers ou une organisation internationale, en vertu d'une disposition nationale ou internationale auquel il est soumis, il doit informer le Responsable de traitement de cette obligation juridique avant le traitement, sauf à ce qu'une telle information soit interdite pour des motifs importants d'intérêt public ;
- 2.2.1.6 assurer une étanchéité absolue entre les Données Personnelles du Responsable de traitement, et toute autre donnée ou information dont il pourrait assurer le stockage ou qu'il pourrait traiter pour son propre compte ou pour le compte de tout tiers, notamment d'autres clients non destinataires ;
- 2.2.1.7 prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des Données Personnelles en cours d'exécution des prestations ;
- 2.2.1.8 garantir la confidentialité des Données Personnelles traitées dans le cadre du présent DPA ;
- 2.2.1.9 veiller à ce que les personnes autorisées à traiter les Données Personnelles en vertu des Conditions Générales de Vente i) s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité et ii) reçoivent la formation nécessaire en matière de protection des Données Personnelles.

2.3 Obligations en matière de sécurité des Données Personnelles.

Le Sous-traitant s'engage à mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités ainsi que des risques.

2.4 Obligations en matière de violation de Données Personnelles

2.4.1 Le Sous-traitant informe le Responsable de traitement de toute atteinte à la sécurité ayant des conséquences directes ou indirectes sur les Données Personnelles et/ou susceptible d'entraîner accidentellement la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des Données Personnelles et ce, dans les trente-six (36) heures après en avoir pris connaissance. Cette information sera adressée par courrier électronique et sera accompagnée de toute documentation utile afin de permettre au Responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente et aux personnes concernées, le cas échéant.

2.4.2 Dans l'hypothèse où le Sous-traitant serait dans l'impossibilité de fournir toutes les informations en même temps, les informations pourront être communiquées de manière échelonnée.

2.4.3 Le Responsable de traitement demande au Sous-traitant de prendre toutes les mesures qu'il jugera nécessaires ou utiles pour sécuriser les données traitées pour le compte du Responsable de traitement et minimiser les éventuelles conséquences indésirables pour la personne concernée.

2.4.4 Il est entendu entre les Parties que les « atteintes à la sécurité » n'incluront pas les tentatives vaines ou les activités n'affectant pas la sécurité des Données Personnelles du Responsable de traitement, et notamment les tentatives infructueuses de connexion, requêtes ping, balayages de ports, attaques par déni de service et autres attaques de réseau sur des pare-feux ou des systèmes en réseau.

2.5 Obligations relatives à la conservation des Données Personnelles

2.5.1 Conformément à son devoir de conseil, il appartient au Sous-traitant de proposer au Responsable de traitement des règles de purge adéquates, en fonction de la nature des Données Personnelles et de la finalité du traitement.

2.5.2 En tout état de cause, le Responsable de traitement a la possibilité de supprimer automatiquement les Données Personnelles de chaque campagne réalisée pendant la durée des Conditions Générales de Vente et ce, de façon automatique, dans un délai qu'il peut paramétrer : un mois, deux mois, trois mois, six mois ou douze mois à compter de la date de fin de campagne. Il relève ainsi de la responsabilité du Responsable de traitement de l'adapter en fonction de sa politique de rétention de Données Personnelles.

2.6 Obligation de tenir un registre des 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 tel que prévu à l'article 30-2 du RGPD comprenant :

- Le nom et les coordonnées des éventuels sous-traitants ultérieurs autorisés dans les conditions prévues à l'article 4 ci-après et, le cas échéant, du Délégué à la Protection des Données ;
- Les catégories de traitements effectués pour le compte du Responsable de traitement ;
- Une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
 - la pseudonymisation et le chiffrement des Données Personnelles ;
 - 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 Personnelles 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.

3. ASSISTANCE DU SOUS-TRAITANT

3.1 En cas d'exercice de leurs droits sur leur Données Personnelles par des personnes concernées directement auprès du Sous-traitant, le Sous-traitant devra adresser ces demandes dès réception par courrier électronique. La responsabilité du Sous-traitant ne sera pas engagée si le Responsable de traitement ne répond pas correctement ou en temps utile à la demande de la personne concernée, ou si le Responsable de traitement ne répond pas du tout aux sollicitations de la personne concernée.

3.2 Dans la mesure du possible, le Sous-traitant s'engage à aider raisonnablement le Responsable de traitement à s'acquitter de ses obligations en cas 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 Personnelles, droit de ne pas faire l'objet d'une décision individuelle automatisée y compris le profilage) et s'engage, à cet égard, à transmettre dans les plus brefs délais au Responsable de traitement les éléments nécessaires pour permettre au Responsable de traitement de répondre aux demandes et à mettre en œuvre les mesures nécessaires pour donner suite à toutes demandes notamment de rectification, de limitation, d'opposition ou de portabilité.

3.3 Par ailleurs, le Sous-traitant s'engage à aider le Responsable de traitement pour la réalisation le cas échéant des analyses d'impact relatives à la protection des Données Personnelles et, au besoin, pour la consultation préalable de l'autorité de contrôle.

3.4 L'assistance prévue aux articles 3.2 et 3.3 du DPA ne devra être fournie que dans la mesure où i) le Responsable de traitement ne peut accéder à l'information concernée par d'autres moyens, ii) ladite information est disponible pour le Sous-traitant et iii) la demande nécessite moins de deux (2) heures de prestations au sein des équipes du Sous-traitant. Dans le cas contraire, le Responsable de traitement s'engage à rembourser tous les coûts et frais engagés par le Sous-traitant dans la fourniture de cette assistance.

4. SOUS-TRAITANCE ULTÉRIEURE

4.1 Le Responsable de traitement reconnaît et accepte que le Sous-traitant fasse appel à des prestataires, dit un « sous-traitant ultérieur », mentionnés dans l'Annexe 2 au présent DPA dans le cadre de l'exécution des Conditions Générales de Vente.

4.2 Le Sous-traitant devra notifier le Responsable de traitement de tout remplacement ou ajout sur la liste des sous-traitants ultérieurs. Le Responsable de traitement pourra émettre des objections sous dix (10) jours après la réception de l'avis du Sous-traitant.

4.3 Toute objection doit être adressée par écrit au Sous-traitant accompagnée des raisons détaillées du refus. Si le Sous-traitant exige toujours un changement du/des sous-traitants ultérieurs, le Sous-traitant fournira au Responsable de traitement au moins une proposition alternative, incluant tous coûts supplémentaires à la charge du Responsable de traitement pour sa mise en œuvre.

4.4 S'il engage des prestataires pour collecter, traiter et/ou utiliser des Données Personnelles au nom du Responsable de traitement, le Sous-traitant s'assurera du respect des conditions ci-après :

4.4.1 le contrat de sous-traitance reprendra en substance les dispositions de protection des données établies entre le Responsable de traitement et le Sous-traitant dans le présent DPA ;

4.4.2 le Sous-traitant sera responsable de la conduite et de l'exécution de chaque sous-traitant ultérieur, et demeurera l'unique interlocuteur du Responsable de traitement eu égard au traitement des Données Personnelles par le sous-traitant ultérieur.

5. AUDITS

5.1 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 par le Responsable de traitement ou un autre auditeur qu'il a mandaté, à l'exception de la documentation relevant du savoir-faire, du secret des affaires du Sous-traitant ainsi que celle couverte par des accords de confidentialité. Tous les documents, informations ou données, quel qu'en soit le support, confiés par le Sous-traitant au Responsable de traitement ou aux auditeurs, seront considérés et traités comme confidentiels.

5.2 Le Responsable de traitement est en droit de procéder, à ses frais, à un audit technique des services liés exclusivement aux prestations qui lui paraîtrait utile pour constater le respect des obligations précitées.

5.3 Le Responsable de traitement n'exercera pas ses droits d'audit plus d'une fois par période de douze (12) mois, sauf (i) si et lorsque cela est requis par instruction d'une autorité compétente en matière de protection des données ou toute autre instance régulatrice ayant compétence sur le Responsable de traitement ; ou si (ii) le Responsable de traitement estime qu'un autre audit est nécessaire en raison d'une atteinte avérée à la sécurité subie par le Sous-traitant.

5.4 Le Responsable de traitement notifiera le Sous-traitant dans un délai raisonnable qui ne sera en aucun cas inférieur à trente (30) jours sauf s'il existe un besoin urgent d'effectuer l'audit plus rapidement. L'audit ne pourra pas dépasser une durée de quatre (4) heures ouvrées pendant les heures habituelles de travail du Sous-traitant de manière à ne pas générer de gêne dans l'activité du Sous-traitant. Par ailleurs, le Sous-traitant pourra conditionner l'audit à la signature d'un accord de confidentialité eu égard aux données d'autres clients et aux mesures techniques et organisationnelles mises en œuvre. Le Responsable de traitement ne pourra pas désigner un auditeur tiers concurrent du Sous-traitant.

5.5 Le Sous-traitant s'engage à apporter son concours de bonne foi et de manière diligente à toute enquête ou audit qui pourrait être ainsi diligentée et à mettre en œuvre, à ses frais, les mesures correctives nécessaires en cas de non-conformité par rapport à ses obligations, et ce, dans un délai préalablement et conjointement défini par les Parties.

6. RESPONSABILITÉ

6.1 Vis-à-vis du Responsable de traitement. Le Responsable de traitement et le Sous-traitant conviennent expressément que, sous respect des dispositions de l'article 9 des Conditions Générales de Vente, le Sous-traitant sera responsable vis-à-vis du Responsable de traitement pour toute violation effective du Sous-traitant à ses obligations décrites dans le présent DPA et prouvée par le Responsable de traitement.

6.2 Vis-à-vis d'une autorité de contrôle (article 82 paragraphe 2 et 3 du RGPD). Le Responsable de traitement sera seul responsable envers toute autorité de contrôle si la violation du présent DPA ou le non-respect des dispositions légales et réglementaires en matière de protection des données à caractère personnel est imputable au seul Responsable de traitement. La responsabilité du Sous-traitant ne pourra être

retenue (i) que s'il a agi en dehors des instructions licites du Responsable de traitement ou contrairement à celles-ci, (ii) qu'en cas de non-respect des dispositions légales et réglementaires en matière de protection des données à caractère personnel qui incombent spécifiquement au Sous-traitant.

6.3 Vis-à-vis d'une personne concernée (article 82 paragraphe 4 et 5 du RGPD). Lorsque le Responsable de traitement et le Sous-traitant sont responsables d'un dommage causé par le traitement, chacun est tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective. Lorsque l'une des Parties a réparé totalement le dommage subi, elle est en droit de réclamer auprès de l'autre Partie la part de la réparation correspondant à la part de responsabilité de l'autre Partie dans le dommage, étant entendu que la responsabilité du Sous-traitant vis-à-vis du Responsable de traitement est limitée conformément aux dispositions de l'article 6.1 du présent DPA.

7. IDENTITE ET COORDONNEES DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Le Sous-traitant communique au Responsable de traitement le nom et les coordonnées de son Délégué à la Protection des Données. A été nommé à cet effet Audrey ARBUSA, joignable par courrier électronique via dpo@socialshaker.com.

8. FIN DU CONTRAT

8.1 A l'expiration des Conditions Générales de Vente, pour quelque cause que ce soit, le Sous-traitant devra dans un délai de trente (30) jours, à la demande du Responsable de traitement, détruire les Données Personnelles et toute copie quel qu'en soit le support, sauf à ce qu'il soit tenu de conserver les Données Personnelles en application du droit applicable à la protection des données.

8.2 Le Sous-traitant s'engage à cet effet à fournir une attestation de destruction sur simple demande du Responsable de traitement.

Les présentes dispositions continueront à produire effet et à s'imposer aux Parties tant que le Sous-traitant traitera des Données Personnelles pour le compte du Responsable de traitement.

ANNEXE 1 : CARACTÉRISTIQUES DU TRAITEMENT DE DONNÉES PERSONNELLES

<i>Services fournis</i>	<i>Traitement</i>	<i>Nature du traitement</i>	<i>Finalités</i>	<i>Catégories de Données Personnelles</i>	<i>Catégories de personnes concernées</i>	<i>Durée du traitement</i>
<i>Création de jeux marketing</i>	<i>collecte des données dans le cadre de jeux marketing</i>	<i>hébergement, accès, consultation, utilisation, destruction</i>	<i>animer la clientèle du CLIENT en organisant des jeux marketing</i>	<i>Nom, prénom, âge, adresse email, adresse postale, données de connexion</i>	<i>clients et prospect</i>	<i>pendant toute la durée des Conditions Générales de Vente</i>

ANNEXE 2 : LISTE DES SOUS-TRAITANTS DE SOCIALSHAKER

Selon les prestations souhaitées par le Responsable de traitement, le Sous-traitant peut faire appel aux sous-traitants ultérieurs listés ci-dessous :

Google Cloud Platform :

- Prestations : héberger les données liées aux prestations souscrites au titre des Conditions Générales de Vente
- Données concernées : Données Personnelles mentionnées dans le présent DPA
- Durée de conservation : durée de conservation indiquée par le Responsable de traitement, sauf demande de suppression et sauf expiration/résiliation des Conditions Générales de Vente
- Lieu de traitement : Union Européenne

CloudFlare :

- Prestations : Sécuriser l'accès aux services Web de SOCIALSHAKER
- Données concernées : Données Personnelles mentionnées dans le présent DPA
- Durée de conservation : durée de conservation indiquée par le Responsable de traitement, sauf demande de suppression et sauf expiration/résiliation des Conditions Générales de Vente
- Lieu de traitement : États-Unis
- Garanties prévues pour encadrer les transferts hors Union européenne : Clauses contractuelles types rédigées par la Commission européenne

MongoDB Atlas :

- Prestations : Fournir le service d'accès aux Données Personnelles liées aux prestations souscrites au titre des Conditions Générales de Vente
- Données concernées : Données Personnelles mentionnées dans le présent DPA
- Durée de conservation : durée de conservation indiquée par le Responsable de traitement, sauf demande de suppression et sauf expiration/résiliation des Conditions Générales de Vente

- Lieu de traitement : Union Européenne

Sendgrid :

- Prestations : Provider d'emailing
- Données concernées : Données Personnelles mentionnées dans le présent DPA
- Durée de conservation : durée de conservation indiquée par le Responsable de traitement, sauf demande de suppression et sauf expiration/résiliation des Conditions Générales de Vente
- Lieu de traitement : États-Unis
- Garanties prévues pour encadrer les transferts hors Union européenne : Clauses contractuelles types rédigées par la Commission européenne