Conditions Générales d'Utilisation (CGU) et Conditions Générales de Vente (CGV) de Prospectia

Dernière mise à jour : 14 août 2024

Table des matières

1. Objet

Les présentes Conditions Générales d'Utilisation (CGU) et Conditions Générales de Vente (CGV) ont pour objet de définir les modalités et conditions dans lesquelles la société Prospectia, immatriculée au Registre du Commerce et des Sociétés de Toulouse sous le numéro 929 708 808, dont le siège social est situé au 1 Rue Traversière, 31450 Baziège, propose à ses clients des services de prospection personnalisée.

Ces services incluent, sans s'y limiter :

- La collecte, l'enrichissement et l'optimisation des bases de données fournies par les clients.
- La création de messages commerciaux sur mesure, adaptés aux besoins spécifiques du client, en utilisant des techniques avancées d'intelligence artificielle.
- L'envoi de ces messages via des canaux de communication électroniques tels que les SMS, les WhatsApp et les e-mails, directement sur les dispositifs ou adresses électroniques des clients ou de leurs collaborateurs.

L'objectif principal des présentes CGU/CGV est d'encadrer les droits et obligations de Prospectia et de ses clients dans le cadre de l'utilisation des services de prospection proposés. Elles visent également à assurer la transparence des conditions de traitement des données personnelles et à préciser les conditions tarifaires applicables aux services.

En acceptant les présentes CGU/CGV, le client reconnaît avoir pris connaissance de l'ensemble des informations relatives aux services proposés et s'engage à respecter les obligations définies par ces conditions.

2. Acceptation des CGU/CGV

L'acceptation des présentes Conditions Générales d'Utilisation (CGU) et Conditions Générales de Vente (CGV) est un préalable obligatoire à toute utilisation des services proposés par Prospectia. Cette acceptation est formalisée de manière expresse par la signature du devis correspondant aux services commandés par le client.

En signant le devis, le client déclare :

- Avoir pris connaissance des présentes CGU/CGV dans leur intégralité.
- Comprendre et accepter l'ensemble des termes et conditions y figurant, sans restriction ni réserve.

Cette acceptation conditionne l'accès aux services de Prospectia, y compris la collecte, le traitement et l'envoi des messages de prospection. En cas de désaccord avec les termes des présentes CGU/CGV, le client est invité à ne pas utiliser les services de Prospectia.

Les présentes CGU/CGV sont applicables à toutes les prestations fournies par Prospectia, sauf accord spécifique et écrit entre les parties stipulant des conditions différentes.

L'acceptation des CGU/CGV inclut également l'adhésion aux politiques de confidentialité et de traitement des données personnelles de Prospectia, lesquelles font partie intégrante des présentes conditions.

Enfin, toute modification ultérieure des CGU/CGV sera notifiée au client par tout moyen approprié, et l'utilisation continue des services par le client après cette notification vaudra acceptation des nouvelles conditions.

3. Services proposés

Prospectia propose des services de prospection personnalisée utilisant des technologies avancées, notamment l'intelligence artificielle, pour maximiser l'efficacité des campagnes de communication de ses clients. Les services offerts par Prospectia incluent les étapes suivantes :

3.1. Collecte et enrichissement des bases de données

Le client fournit à Prospectia une base de données contenant les informations nécessaires à la prospection. Prospectia procède à l'enrichissement et à l'optimisation de ces données, afin de garantir une meilleure précision et pertinence des messages de prospection.

3.2. Création de messages commerciaux personnalisés

Prospectia utilise des modèles d'intelligence artificielle pour générer des messages commerciaux sur mesure. Ces messages sont adaptés aux objectifs et besoins spécifiques du client, prenant en compte des facteurs tels que le public cible, les préférences des destinataires, et le contenu promotionnel souhaité.

3.3. Validation des messages par le client

Avant tout envoi, Prospectia soumet au client les messages types pour validation. Cette étape garantit que le contenu des messages correspond parfaitement aux attentes du client et respecte les normes de communication définies par celui-ci.

3.4. Envoi des messages

Après validation, Prospectia procède à l'envoi des messages via les canaux de communication convenus (SMS, WhatsApp ou e-mail). Les messages sont envoyés directement sur le téléphone portable, le WhatsApp ou l'adresse e-mail du client ou de ses collaborateurs, selon les modalités choisies.

3.5. Suivi et reporting

Prospectia propose un service de suivi et de reporting visant à évaluer l’efficacité des campagnes de prospection menées pour le client. Ce service est conçu pour offrir une vue d’ensemble des performances de la campagne et pour identifier les opportunités d’amélioration pour les futures campagnes.

3.5.1. Collecte des retours

Contrairement à certains services de prospection instantanée, Prospectia n'a pas accès en temps réel aux retours générés par les campagnes de prospection. Au lieu de cela, un suivi est effectué un mois après la fin de la campagne. Durant cette période, le client collecte les retours et résultats de la campagne (réponses des prospects, engagements, ventes, etc.) de manière autonome.

3.5.2. Analyse et bilan chiffré

Un mois après la fin de la campagne, Prospectia prend contact avec le client pour recueillir tous les retours et données collectées durant la campagne. Ces informations sont ensuite analysées par Prospectia pour établir un bilan chiffré. Ce bilan comprend :

- Le nombre total de réponses reçues.
- Le taux d'engagement des prospects.
- Les conversions réalisées (si disponibles).
- Toute autre donnée pertinente que le client aura partagée.

3.5.3. Restitution du rapport

Après l'analyse, Prospectia présente au client un rapport détaillé, incluant des statistiques et des recommandations pour optimiser les futures campagnes. Ce rapport vise à fournir une compréhension claire des résultats obtenus et à proposer des ajustements stratégiques pour améliorer les performances des prochaines campagnes.

3.5.4. Recommandations

Sur la base du bilan chiffré, Prospectia propose des recommandations pour ajuster les messages, les cibles ou les stratégies utilisées, afin d'optimiser les résultats des futures campagnes. Ces recommandations peuvent inclure des suggestions sur le moment idéal pour envoyer les messages, des ajustements dans la segmentation des cibles, ou des conseils pour améliorer le contenu des messages.

Ce processus de suivi et de reporting différé permet à Prospectia d'offrir une analyse approfondie et stratégique des campagnes de prospection, assurant ainsi une amélioration continue des performances de ses services pour le client.

3.6. Support client

Prospectia s'engage à fournir un service client complet et personnalisé tout au long de la prestation. Étant donné que Prospectia prend en charge l'ensemble du processus de prospection, le client n'a pas besoin de gérer une interface complexe. Le support client est conçu pour répondre à toutes les questions et besoins du client de manière réactive et efficace.

3.6.1. Assistance personnalisée

Le client peut contacter directement l'équipe de Prospectia pour toute question relative à la prestation, que ce soit pour des précisions sur le déroulement de la campagne, des ajustements à apporter, ou des informations supplémentaires sur les services. Cette assistance est disponible tout au long de la collaboration, afin d'assurer que les besoins du client soient pleinement satisfaits.

3.6.2. Support pour l'envoi des SMS

Bien que le client n'ait pas à gérer une interface pour la majorité des services, une interface simplifiée est mise à disposition pour l'envoi des SMS. Prospectia offre un accompagnement pour l'utilisation de cette interface, incluant des explications sur son fonctionnement et une assistance en cas de difficulté.

3.6.3. Modes de contact

Le client peut contacter Prospectia via différents canaux :

- **Par téléphone** : Un numéro direct est mis à disposition pour des réponses rapides et des échanges en temps réel.
- **Par e-mail** : Le client peut envoyer ses demandes ou questions par e-mail, avec l'assurance d'une réponse dans les meilleurs délais.
- **En rendez-vous** : Si nécessaire, Prospectia peut organiser des réunions en visioconférence pour discuter de la campagne ou traiter des questions spécifiques.

3.6.4. Réactivité et disponibilité

Prospectia s'engage à répondre aux demandes du client dans les plus brefs délais, en priorisant les urgences liées à la campagne en cours. Le support client est conçu pour être réactif et proactif, anticipant les besoins du client et résolvant les problèmes avant qu'ils n'affectent la campagne.

En offrant un support client complet et accessible, Prospectia garantit que ses clients bénéficient d'une expérience fluide et sans souci, leur permettant de se concentrer sur leurs objectifs de prospection sans avoir à se soucier des aspects techniques ou logistiques.

4. Processus de commande et paiement

Le processus de commande et de paiement chez Prospectia est structuré en plusieurs étapes clés afin d'assurer une prestation de qualité et une relation transparente avec le client. Voici les étapes détaillées :

4.1. Étape 1 : Signature du devis

Le processus débute par la signature d’un devis détaillant les services à fournir par Prospectia. Ce devis inclut une description des prestations, les quantités de messages à envoyer, ainsi que le coût total de la prestation. La signature du devis par le client formalise l'accord entre les parties et marque le début de la collaboration.

4.2. Étape 2 : Paiement de l'acompte de 40 %

Après la signature du devis, le client est tenu de verser un acompte correspondant à 40 % du montant total indiqué. Cet acompte est une condition préalable au commencement des travaux par Prospectia, incluant la préparation des bases de données et la génération des messages de prospection. Le paiement de cet acompte valide définitivement la commande.

4.3. Étape 3 : Envoi de la base de données par le client

Une fois l'acompte reçu, le client doit fournir à Prospectia la base de données nécessaire pour la prospection. Cette base de données contient les informations des contacts ciblés pour la campagne (numéros de téléphone, adresses e-mail, etc.). Prospectia procède ensuite à l'enrichissement et à l'optimisation de cette base de données.

4.4. Étape 4 : Validation du message type

Prospectia génère un ou plusieurs messages types en fonction des objectifs définis. Ces messages sont soumis au client pour validation. Le client peut demander des modifications afin que le message corresponde parfaitement à ses attentes. La validation du message type est essentielle avant le déploiement de la campagne.

4.5. Étape 5 : Livraison des messages

Une fois le message type validé, Prospectia procède à l'envoi des messages via SMS, WhatsApp ou e-mail, conformément aux termes convenus. Les messages sont livrés directement sur le téléphone portable, le WhatsApp ou la boîte mail du client ou de ses collaborateurs. L'envoi peut être planifié en fonction des préférences du client (horaire, date, etc.).

4.6. Étape 6 : Paiement du solde de 60 %

Après l'envoi et la confirmation de la bonne réception des messages, le client est tenu de régler le solde restant de 60 % du montant total. Le paiement du solde marque la clôture de la prestation. Le paiement doit être effectué dans les délais indiqués sur la facture émise par Prospectia.

4.7. Modalités de paiement

Le paiement peut être effectué par virement bancaire ou tout autre moyen accepté par Prospectia et précisé dans le devis. Les paiements sont effectués en euros (€), et les prix s'entendent hors taxes (HT). Le non-paiement du solde dans les délais impartis peut entraîner des pénalités de retard et, le cas échéant, la suspension des services fournis par Prospectia.

En respectant ces étapes, Prospectia garantit une prestation structurée et conforme aux attentes du client, tout en assurant la transparence et la clarté dans les relations commerciales.

4.8. Tarification

La tarification des services de Prospectia est clairement définie dans le devis signé par le client. Les tarifs sont calculés en fonction du volume de messages à envoyer (SMS, WhatsApp ou e-mails) et sont structurés de manière dégressive pour encourager les envois de grandes quantités. Voici les détails de la tarification applicable :

4.8.1. Tarification des SMS

- **De 500 à 3000 SMS** : Le tarif est de **1,34 € HT par SMS**. Ce tarif s'applique pour les campagnes de prospection envoyant un nombre de SMS compris entre 500 et 3000 unités.
- **À partir de 3000 SMS** : Le tarif est réduit à **1,07 € HT par SMS** pour les campagnes dépassant les 3000 SMS. Cette tarification dégressive vise à offrir un coût plus avantageux pour les envois de masse.

4.8.2. Tarification des e-mails et WhatsApp

- **À partir de 500 e-mails ou WhatsApp :** Le tarif est de **0,70 € HT par e-mail ou WhatsApp.** Ce tarif s'applique dès que la campagne de prospection comprend au moins 500 e-mails ou WhatsApp.

4.8.3. Tarification tout compris

Les tarifs indiqués incluent l'ensemble des services liés à l'envoi des SMS, des WhatsApp et des e-mails, tels que la collecte et l'enrichissement des données, la création des messages, et le suivi post-campagne. Il n'y a pas de frais cachés ou supplémentaires, sauf si des services additionnels sont demandés par le client et acceptés par Prospectia.

5. Confidentialité et protection des données

La confidentialité et la protection des données sont des priorités pour Prospectia, qui s'engage à respecter la législation en vigueur, notamment le Règlement Général sur la Protection des Données (RGPD). Voici les principes et mesures adoptés par Prospectia pour assurer la sécurité et la confidentialité des données personnelles traitées :

5.1. Collecte des données

Prospectia collecte des données personnelles dans le cadre de ses services de prospection. Ces données sont principalement fournies par le client et peuvent inclure des noms, prénoms, adresses électroniques, numéros de téléphone, et autres informations pertinentes pour la prospection. Le client est responsable de la légalité des données fournies et de leur conformité avec le RGPD.

5.2. Utilisation des données

Les données collectées sont utilisées exclusivement pour les besoins des services commandés par le client. Cela inclut la création de messages personnalisés, l'envoi de ces messages, et le suivi des campagnes de prospection. Prospectia ne partage jamais les données d'un client avec un autre client ou une tierce partie non impliquée dans la prestation de services, sauf accord exprès du client ou obligation légale.

5.3. Sous-traitance des données

Prospectia peut faire appel à des sous-traitants pour certaines opérations, comme l'hébergement des bases de données et des serveurs. Ces sous-traitants, sélectionnés avec soin, sont tenus de respecter les mêmes obligations de confidentialité et de protection des données que Prospectia. Les principaux sous-traitants comprennent :

- Scaleway (France) pour l'hébergement des bases de données.
- Contabo (Allemagne) pour l'hébergement des serveurs.
- OpenAI (Irlande), Scaleway (France), ou Infomaniak (Suisse) pour l'hébergement des moteurs d'inférence.

Tous les sous-traitants sont tenus de se conformer aux obligations du RGPD et ne peuvent utiliser les données personnelles que dans le cadre des services définis par Prospectia.

5.4. Mesures de sécurité

Prospectia met en œuvre des mesures techniques et organisationnelles appropriées pour protéger les données personnelles contre toute forme de perte, d'accès non autorisé, de divulgation ou d'altération. Ces mesures comprennent :

- Le chiffrement des données lors de leur transmission et de leur stockage.
- L'anonymisation des données dans certains cas, notamment lors de l'utilisation de moteurs d'inférence.
- La restriction de l'accès aux données uniquement aux personnes autorisées.

5.5. Conservation des données

Les données personnelles sont conservées uniquement pendant la durée nécessaire aux fins pour lesquelles elles ont été collectées, conformément aux obligations légales et contractuelles. À l'issue de cette période, les données sont soit supprimées, soit anonymisées de manière sécurisée, sauf obligation légale de les conserver plus longtemps.

5.6. Responsable du traitement et Délégué à la Protection des Données (DPO)

Le responsable du traitement des données personnelles chez Prospectia est Monsieur Thomas Peyre. Le Délégué à la Protection des Données (DPO) est Monsieur Enzo Blanchon. Ils peuvent être contactés aux adresses e-mail suivantes pour toute question relative à la protection des données :

- Thomas Peyre : peyrethomas@gmail.com
- Enzo Blanchon : blanchonenzo@gmail.com

5.7. Droits des personnes concernées

Conformément au RGPD, les personnes concernées par les traitements de données mis en œuvre par Prospectia disposent de plusieurs droits, notamment :

- Droit d'accès : Droit de savoir si des données personnelles les concernant sont traitées par Prospectia, et de demander une copie de ces données.
- Droit de rectification : Droit de demander la correction de données inexactes ou incomplètes.
- Droit à l'effacement : Droit de demander la suppression des données personnelles, sous réserve des obligations légales de conservation.
- Droit à la limitation du traitement : Droit de demander la limitation du traitement des données dans certains cas.
- Droit d'opposition : Droit de s'opposer au traitement des données pour des raisons légitimes.
- Droit à la portabilité : Droit de recevoir les données personnelles dans un format structuré et couramment utilisé, et de les transmettre à un autre responsable de traitement.

Ces droits peuvent être exercés en contactant le DPO aux adresses e-mail mentionnées ci-dessus. Prospectia s'engage à répondre aux demandes dans les délais légaux.

5.8. Notification en cas de violation de données

En cas de violation des données personnelles, Prospectia notifiera cette violation à l'autorité de contrôle compétente et, si nécessaire, aux personnes concernées, conformément aux exigences du RGPD.

5.9. Transferts de données hors de l'Union Européenne

Les données personnelles traitées par Prospectia sont principalement hébergées au sein de l'Union Européenne. Dans les cas où un transfert de données en dehors de l'UE est nécessaire, Prospectia s'engage à mettre en place des garanties appropriées, telles que des clauses contractuelles types, afin d'assurer un niveau de protection adéquat des données.

En adoptant ces mesures, Prospectia garantit à ses clients que leurs données personnelles sont protégées conformément aux normes les plus strictes de confidentialité et de sécurité.

6. Livraison des services

La livraison des services par Prospectia s'effectue conformément aux modalités définies dans le devis signé par le client. Cette livraison englobe plusieurs étapes cruciales visant à garantir que les services fournis répondent aux attentes du client et sont exécutés dans les délais convenus.

6.1. Validation préalable

Avant toute livraison, Prospectia soumet au client le message type généré par ses systèmes d'intelligence artificielle. Cette validation est une étape obligatoire, permettant au client de s'assurer que le contenu est conforme à ses attentes et aux objectifs définis pour la campagne de prospection. Aucune livraison de message ne sera effectuée sans l'approbation explicite du client.

6.2. Modes de livraison

Prospectia propose plusieurs modes de livraison pour les messages de prospection, adaptés aux besoins spécifiques de chaque client. Ces modes de livraison incluent des options pour l'envoi des SMS, des WhatsApp et des e-mails, avec des outils adaptés pour assurer une gestion efficace des campagnes.

6.2.1. Interface de livraison pour les SMS

Pour les campagnes de prospection par SMS, Prospectia met à disposition du client une interface dédiée. Cette interface permet au client de gérer directement l'envoi des SMS en suivant un processus simple et intuitif.

Prospectia fournit un support pour l'utilisation de cette interface, garantissant que le client est à l'aise avec l'outil et peut en tirer le meilleur parti pour ses campagnes de prospection.

6.2.2. Livraison par e-mail et WhatsApp

Pour les campagnes de prospection par e-mail et WhatsApp, Prospectia prend en charge l'intégralité du processus d'envoi. Les messages sont envoyés directement depuis la boîte mail ou le WhatsApp du client. Cela permet de maintenir la relation de confiance avec les destinataires en utilisant une adresse familière. Prospectia aide à personnaliser les e-mails et les WhatsApp, et à respecter les normes anti-spam, tout en assurant la sécurité des données. Ce mode de livraison garantit une continuité de la communication avec une gestion optimisée de la campagne.

6.3. Planning de livraison

Prospectia travaille en étroite collaboration avec le client pour définir le planning de livraison des messages. Ce planning prend en compte les meilleures pratiques en matière de prospection, telles que les horaires optimaux d'envoi pour maximiser l'impact des messages. Le calendrier de livraison est validé par le client avant l'envoi.

6.4. Confirmation de livraison

Après l'envoi des messages, Prospectia fournit au client une confirmation de livraison. Cette confirmation inclut des détails sur les messages envoyés, tels que le nombre de SMS, de WhatsApp ou d'e-mails livrés, et les éventuelles erreurs de transmission. Ce rapport permet au client de vérifier que la campagne a été exécutée conformément aux attentes.

6.5. Suivi et reporting

Prospectia propose un service de suivi et de reporting pour évaluer l'efficacité des campagnes de prospection. Ce service est conçu pour offrir une analyse détaillée des performances, mais il est important de noter que les retours ne sont pas disponibles en temps réel.

6.5.1. Collecte des retours

Les retours des campagnes de prospection ne sont pas suivis en temps réel par Prospectia. Un mois après la fin de la campagne, Prospectia contacte le client pour collecter tous les retours et résultats obtenus (réponses, engagements, conversions, etc.). Pendant ce mois, le client est responsable de suivre les retours en interne.

6.5.2. Analyse et bilan chiffré

Après avoir collecté les retours du client, Prospectia effectue une analyse complète des résultats. Un bilan chiffré est ensuite établi, comprenant le nombre de réponses reçues, le taux d'engagement, et d'autres métriques clés. Cette analyse aide à comprendre l'impact de la campagne et à identifier les points d'amélioration.

6.5.3. Restitution du rapport

Une fois l'analyse terminée, Prospectia fournit au client un rapport détaillé, incluant les statistiques de la campagne et des recommandations pour optimiser les futures campagnes. Ce rapport est conçu pour offrir une vision claire des performances et guider les décisions stratégiques.

Ce suivi différé permet à Prospectia d'offrir une analyse approfondie et de proposer des ajustements pour améliorer l'efficacité des futures campagnes de prospection.

6.6. Gestion des incidents

En cas de problème lors de la livraison (ex. : échec de l'envoi, erreurs techniques, etc.), Prospectia s'engage à informer immédiatement le client et à prendre toutes les mesures nécessaires pour résoudre l'incident. Cela peut inclure un nouvel envoi des messages, la correction des erreurs, ou toute autre action convenue avec le client pour minimiser l'impact de l'incident.

6.7. Conditions spécifiques

Certaines conditions spécifiques de livraison peuvent être convenues entre Prospectia et le client, notamment en ce qui concerne les volumes importants de messages, les contraintes temporelles strictes, ou les exigences particulières de confidentialité. Ces conditions doivent être explicitement mentionnées dans le devis ou dans un avenant au contrat.

En assurant une livraison rigoureuse et personnalisée de ses services, Prospectia garantit à ses clients une exécution fiable de leurs campagnes de prospection, avec un suivi détaillé pour maximiser les résultats.

7. Responsabilité

Les présentes Conditions Générales d'Utilisation (CGU) et Conditions Générales de Vente (CGV) définissent les limites de la responsabilité de Prospectia ainsi que celle du client dans le cadre de l'utilisation des services de prospection proposés.

7.1. Responsabilité de Prospectia

Prospectia s'engage à fournir ses services avec le plus grand soin, en conformité avec les pratiques professionnelles et les obligations légales en vigueur. Toutefois, la responsabilité de Prospectia est limitée aux dommages directs prouvés, résultant d'une faute avérée de sa part, dans le cadre de l'exécution des services contractés.

- Limitation de responsabilité : Prospectia ne pourra en aucun cas être tenue responsable des dommages indirects, tels que la perte de profit, la perte de clientèle, les perturbations des affaires ou les réclamations de tiers, découlant de l'utilisation ou de l'incapacité à utiliser les services fournis.
- Obligation de moyens : Prospectia s'engage à mettre en œuvre tous les moyens nécessaires pour assurer la bonne exécution des services, mais elle ne garantit pas l'atteinte de résultats spécifiques, notamment en termes de taux de réponse ou de conversion des campagnes de prospection.

7.2. Responsabilité du client

Le client reconnaît être seul responsable des données qu'il fournit à Prospectia pour l'exécution des services de prospection, ainsi que de l'utilisation qui en est faite.

- Légalité des données : Le client garantit que les données transmises à Prospectia sont collectées et utilisées en conformité avec la législation en vigueur, notamment le RGPD. Le client s'engage à obtenir tous les consentements nécessaires auprès des personnes concernées avant de transmettre leurs données à Prospectia.
- Utilisation des services : Le client est responsable de l'utilisation des services de prospection et des conséquences qui en découlent. Il s'engage à ne pas utiliser les services de Prospectia à des fins illégales, frauduleuses, ou contraires à l'ordre public.
- Indemnisation : Le client s'engage à indemniser Prospectia de toute réclamation, dommage, perte ou dépense, y compris les frais d'avocat raisonnables, résultant de l'utilisation des services par le client en violation des présentes CGU/CGV ou de la législation applicable.

7.3. Cas de force majeure

Aucune des parties ne sera tenue responsable en cas de non-exécution ou de retard dans l'exécution de l'une de ses obligations, si cette non-exécution ou ce retard est dû à un cas de force majeure. Sont notamment considérés comme cas de force majeure les catastrophes naturelles, les grèves, les guerres, les épidémies, les pannes informatiques majeures, les interruptions des réseaux de communication, ou toute autre circonstance échappant au contrôle raisonnable des parties.

En cas de survenance d'un événement de force majeure, la partie concernée devra en informer l'autre partie dans les meilleurs délais et les deux parties conviendront des mesures à prendre pour atténuer les effets de cet événement.

7.4. Exclusions spécifiques

Prospectia ne saurait être tenue responsable des conséquences résultant :

- D'une mauvaise utilisation des services par le client, notamment l'envoi de messages à des destinataires non consentants.
- D'un défaut de fonctionnement ou d'une interruption des services imputables à des tiers, tels que les prestataires de télécommunications ou les hébergeurs de données.
- De la non-livraison des messages en raison d'informations incorrectes fournies par le client (ex. : numéros de téléphone ou adresses e-mail erronés).

7.5. Assurance

Prospectia déclare être couverte par une assurance responsabilité civile professionnelle, pour les dommages qui pourraient être causés dans le cadre de l'exécution de ses services. Le client est invité à souscrire une assurance couvrant ses propres risques, notamment ceux liés à l'utilisation des données personnelles dans le cadre de campagnes de prospection.

En résumé, les présentes CGU/CGV encadrent la responsabilité des parties de manière équilibrée, en définissant clairement les obligations et les risques associés à l'utilisation des services de Prospectia. Le respect mutuel de ces responsabilités est essentiel pour le succès des campagnes de prospection.

8. Durée et résiliation

Les présentes Conditions Générales d'Utilisation (CGU) et Conditions Générales de Vente (CGV) régissent la relation contractuelle entre Prospectia et ses clients pour une durée déterminée par le devis signé. Elles prévoient également les conditions dans lesquelles le contrat peut être résilié, que ce soit à l'initiative du client ou de Prospectia.

8.1. Durée du contrat

La durée du contrat entre Prospectia et le client est définie dans le devis signé par les deux parties. Sauf mention contraire dans le devis, le contrat prend effet à la date de la signature du devis par le client et se termine une fois que toutes les obligations des parties ont été exécutées, notamment après la livraison des services et le paiement intégral du montant dû par le client.

8.2. Renouvellement

Si le client souhaite renouveler les services de Prospectia après l'exécution du contrat initial, un nouveau devis devra être établi et signé. Les présentes CGU/CGV s'appliqueront également à tout contrat renouvelé, sauf si des conditions spécifiques sont stipulées dans le nouveau devis.

8.3. Résiliation à l'initiative du client

Le client peut résilier le contrat à tout moment avant la livraison des services, sous réserve des conditions suivantes :

- Résiliation avant validation du message type : Si le client résilie le contrat avant la validation du message type, l'acompte de 40 % déjà versé reste acquis à Prospectia à titre d'indemnité pour les travaux préparatoires effectués.
- Résiliation après validation du message type : Si la résiliation intervient après la validation du message type, le client est tenu de payer la totalité du montant convenu dans le devis, même si les services ne sont pas intégralement livrés. Prospectia pourra, à sa discrétion, décider de ne pas exiger le paiement du solde si les services n'ont pas été livrés.

8.4. Résiliation à l'initiative de Prospectia

Prospectia se réserve le droit de résilier le contrat de plein droit, sans préavis, dans les cas suivants :

- Non-paiement des sommes dues : Si le client ne paie pas l'acompte de 40 % ou le solde de 60 % dans les délais convenus, malgré une mise en demeure restée sans réponse pendant 10 jours.
- Violation des obligations contractuelles : Si le client enfreint gravement ses obligations contractuelles, notamment en matière de fourniture de données ou de respect des lois applicables à la prospection commerciale.
- Cas de force majeure : En cas de survenance d'un événement de force majeure rendant impossible la poursuite du contrat.

8.5. Effets de la résiliation

En cas de résiliation du contrat, quelle qu'en soit la cause :

- Cessation des services : Prospectia cessera immédiatement la fourniture des services au client.
- Paiement des services rendus : Le client reste redevable du paiement des services rendus jusqu'à la date de la résiliation. Si le solde du montant dû est supérieur aux services rendus, Prospectia facturera au client les services effectivement fournis, et le client sera tenu de régler cette facture dans les délais impartis.
- Restitution des données : Sur demande écrite du client, Prospectia s'engage à restituer ou détruire les données fournies par le client, conformément aux modalités prévues à l'article 5.6 des présentes CGU/CGV.

8.6. Clause de survie

Les dispositions des présentes CGU/CGV qui, par leur nature, survivent à la résiliation du contrat (telles que la confidentialité, la responsabilité, et la protection des données) continueront de produire leurs effets après la résiliation, quelle qu'en soit la cause.

En structurant les conditions de durée et de résiliation de manière claire, Prospectia s'assure que les deux parties connaissent leurs droits et obligations en cas de fin de contrat, permettant ainsi une gestion sereine de la relation commerciale.

9. Loi applicable et juridiction compétente

Les présentes Conditions Générales d'Utilisation (CGU) et Conditions Générales de Vente (CGV) sont régies par le droit français. Elles encadrent la relation contractuelle entre Prospectia et ses clients, en définissant les droits et obligations de chaque partie.

9.1. Loi applicable

Le contrat entre Prospectia et le client, ainsi que l'ensemble des relations contractuelles qui en découlent, sont exclusivement soumis à la législation française. Cela inclut toutes les dispositions des présentes CGU/CGV, ainsi que les litiges potentiels qui pourraient survenir en rapport avec l'interprétation, l'exécution ou la résiliation du contrat.

9.2. Juridiction compétente

En cas de litige relatif à l'interprétation, l'exécution ou la résiliation du contrat, et à défaut de résolution amiable entre les parties, le différend sera soumis à la compétence exclusive des tribunaux du ressort du siège social de Prospectia, à savoir le Tribunal de Commerce de Toulouse.

Cette attribution de juridiction est acceptée par le client, même en cas de pluralité de défendeurs, d'appel en garantie, ou de procédure d'urgence, que celle-ci soit au fond ou par référé.

9.3. Résolution amiable des litiges

Avant d'engager une procédure judiciaire, les parties s'engagent à tenter de résoudre tout différend de manière amiable. À cette fin, elles se rapprocheront et mettront en œuvre tous les efforts raisonnables pour trouver une solution satisfaisante pour les deux parties. Si le différend n'est pas résolu dans un délai de 30 jours suivant la notification du litige par l'une des parties, celles-ci pourront engager la procédure judiciaire devant les juridictions compétentes.

9.4. Langue du contrat

Les présentes CGU/CGV sont rédigées en langue française, qui sera considérée comme la langue officielle pour toute interprétation ou exécution des conditions contractuelles. En cas de traduction dans une autre langue, la version française prévaudra en cas de divergence ou de contestation.

9.5. Compatibilité internationale

Si le client est situé en dehors de la France, il accepte expressément que les présentes CGU/CGV soient soumises au droit français et que tout litige soit tranché par les tribunaux français compétents, conformément aux dispositions prévues dans cette clause.

En définissant clairement la loi applicable et la juridiction compétente, Prospectia garantit que toutes les parties sont conscientes des règles qui régissent leurs relations contractuelles et du cadre juridique dans lequel les litiges éventuels seront résolus. Cela contribue à une meilleure sécurité juridique pour toutes les parties impliquées.

10. Modification des CGU/CGV

Prospectia se réserve le droit de modifier les présentes Conditions Générales d'Utilisation (CGU) et Conditions Générales de Vente (CGV) à tout moment, afin de les adapter aux évolutions légales, réglementaires, technologiques, ou à toute autre raison jugée nécessaire par la société. Cette clause vise à assurer que les CGU/CGV restent pertinentes et adaptées aux services fournis par Prospectia.

10.1. Procédure de modification

Les modifications des CGU/CGV seront notifiées au client par tout moyen approprié, y compris, mais sans s'y limiter :

- Publication sur le site internet de Prospectia : Les nouvelles CGU/CGV seront mises à disposition sur le site internet de Prospectia, et la date de la dernière mise à jour sera clairement indiquée.
- Notification par e-mail : Prospectia pourra informer directement le client par e-mail des modifications apportées aux CGU/CGV, en fournissant un lien vers les nouvelles conditions.

10.2. Prise d'effet des modifications

Les modifications apportées aux CGU/CGV entreront en vigueur immédiatement après leur publication ou notification, sauf indication contraire spécifiée par Prospectia. La version mise à jour des CGU/CGV s'appliquera automatiquement à toutes les commandes de services passées après la date d'entrée en vigueur des modifications.

10.3. Acceptation des modifications

En continuant à utiliser les services de Prospectia après l'entrée en vigueur des modifications des CGU/CGV, le client accepte les nouvelles conditions sans réserve. Si le client n'accepte pas les modifications apportées, il a la possibilité de résilier son contrat conformément aux dispositions de l'article 8 des présentes CGU/CGV.

10.4. Impact des modifications sur les contrats en cours

Pour les contrats en cours au moment de la modification des CGU/CGV, les nouvelles conditions s’appliqueront automatiquement, sauf si des dispositions particulières ont été convenues entre Prospectia et le client dans le cadre de ce contrat spécifique. Si une modification substantielle des CGU/CGV est jugée défavorable par le client, celui-ci peut demander une résiliation anticipée du contrat, sans pénalité, dans un délai de 30 jours suivant la notification de la modification.

10.5. Consultation des CGU/CGV

Le client est invité à consulter régulièrement les CGU/CGV disponibles sur le site internet de Prospectia, pour rester informé des éventuelles modifications. Prospectia s'engage à conserver un historique des versions des CGU/CGV pour permettre au client de consulter les versions précédentes en cas de besoin.

Cette clause de modification permet à Prospectia de rester flexible et réactive face aux évolutions de son environnement, tout en assurant la transparence et l'information adéquate de ses clients.

Annexes

Les documents suivants sont annexés aux présentes CGU/CGV et en font partie intégrante :

- Annexe 1 : Prospectia - Politique de confidentialité RGPD
- Annexe 2 : Prospectia - Registre simplifié des traitements
- Annexe 3 : Data Processing Agreement (DPA) de Scaleway
- Annexe 4 : Data Processing Addendum (DPA) de OpenAI
- Annexe 5 : Privacy Policy de Contabo
- Annexe 6 : Infomaniak et la protection de vos données personnelles

Annexe 1 : Prospectia - Politique de confidentialité RGPD

Politique de Confidentialité RGPD de Prospectia

Dernière mise à jour : 14 août 2024

Prospectia s'engage à protéger la confidentialité de vos données personnelles et à les traiter conformément aux réglementations applicables, notamment le Règlement Général sur la Protection des Données (RGPD). Cette politique de confidentialité explique quelles données nous collectons, comment nous les utilisons, et quels sont vos droits en tant que personne concernée.

1. Responsable du traitement

Le responsable du traitement des données à caractère personnel est :

- **Nom** : Thomas Peyre
- **Adresse** : 1 Rue Traversière, 31450 Baziège
- **E-mail** : peyrethomas@gmail.com
- **Téléphone** : 06 25 81 18 10

2. Délégué à la protection des données (DPO)

Le DPO de Prospectia est Enzo Blanchon. Vous pouvez le contacter pour toute question relative à la protection de vos données :

- **Nom** : Enzo Blanchon
- **Adresse** : 1 Rue Traversière, 31450 Baziège
- **E-mail** : blanchonenzo@gmail.com
- **Téléphone** : 06 25 81 18 10

3. Données collectées

Prospectia collecte différentes catégories de données personnelles, en fonction de la nature de la relation et des interactions avec le client. Voici les détails sur les types de données que nous collectons :

3.1. Données collectées via le formulaire de contact

Lorsque vous remplissez notre formulaire de contact sur notre site internet ou via tout autre moyen de communication, nous collectons les informations suivantes :

- **Nom et prénom** : Pour pouvoir vous identifier et personnaliser nos échanges.
- **Adresse électronique** : Pour répondre à vos demandes et vous envoyer des informations.
- **Numéro de téléphone** : Pour vous contacter rapidement en cas de besoin.

3.2. Données collectées lors des demandes de devis

Lorsque vous faites une demande de devis, nous collectons des informations supplémentaires nécessaires pour évaluer vos besoins et vous fournir une offre adaptée :

- **Nom et prénom** : Pour identifier le demandeur.
- **Adresse électronique** : Pour l'envoi du devis et d'autres communications.
- **Numéro de téléphone** : Pour des échanges rapides concernant le devis.
- **Adresse postale** : Si nécessaire pour la facturation ou la correspondance.
- **Informations sur votre projet** : Détails concernant le projet pour lequel vous sollicitez nos services, afin de vous proposer une solution personnalisée.

3.3. Données collectées lors de la participation à un évènement

Si vous nous contactez dans le cadre d'un évènement (salon, conférence, etc.), les données suivantes peuvent être collectées :

- **Nom et prénom** : Pour l'identification.
- **Adresse électronique** : Pour l'envoi d'informations relatives à l'évènement ou à nos services.
- **Numéro de téléphone** : Pour faciliter les prises de rendez-vous ou autres communications.
- **Adresse postale** : Si vous souhaitez recevoir de la documentation physique.
- **Souhaits de prise de rendez-vous et d'envoi de documentation** : Informations spécifiques sur vos préférences de contact et les types de documents que vous souhaitez recevoir.
- **Informations sur votre projet** : Pour mieux comprendre vos besoins et vous offrir une réponse adaptée.

3.4. Données collectées lors des campagnes de prospection

Pour la réalisation de campagnes de prospection personnalisées, vous nous fournissez une base de données contenant les informations nécessaires pour contacter vos prospects. Les types de données collectées dans ce cadre peuvent inclure :

- **Nom et prénom des prospects** : Pour personnaliser les messages de prospection.
- **Numéros de téléphone** : Pour l'envoi de SMS et de WhatsApp de prospection.
- **Adresses électroniques** : Pour l'envoi d'e-mails de prospection.
- **Autres informations spécifiques** : Toute autre donnée fournie par le client pour enrichir et cibler les campagnes de prospection, telles que les historiques de contact, préférences, ou informations démographiques.

3.5. Données de navigation sur le site web

Lors de votre visite sur notre site internet, des données de navigation peuvent être collectées automatiquement, telles que :

- **Adresse IP** : Pour identifier la provenance des visites et assurer la sécurité du site.
- **Cookies** : Pour améliorer l'expérience utilisateur, personnaliser les contenus, et analyser le trafic sur le site.

Ces données sont collectées dans le respect des lois applicables et avec votre consentement lorsque cela est nécessaire, notamment pour les cookies.

En collectant ces données, Prospectia s'efforce de fournir un service de haute qualité, adapté aux besoins de ses clients tout en respectant la confidentialité et la sécurité des informations personnelles.

4. Utilisation des données

Les données personnelles collectées par Prospectia sont utilisées dans le cadre strict des services que nous proposons. Nous nous engageons à utiliser vos données de manière transparente, légitime et conforme à vos attentes. Voici comment nous utilisons vos données personnelles :

4.1. Répondre à vos demandes

Les informations que vous nous fournissez via les formulaires de contact, les demandes de devis ou lors d'événements sont utilisées pour :

- **Répondre à vos questions et demandes spécifiques** : Nous utilisons vos coordonnées pour vous contacter et répondre à vos demandes, qu'il s'agisse d'informations sur nos services, de devis, ou de rendez-vous.
- **Fournir des informations supplémentaires** : Si vous avez demandé à recevoir des documents, des brochures ou d'autres informations, nous utilisons vos données pour vous les envoyer.

4.2. Réalisation des campagnes de prospection

Les données que vous nous fournissez pour la prospection sont utilisées pour :

- **Créer et personnaliser les messages de prospection** : Nous utilisons les informations sur vos prospects pour générer des messages adaptés, qui répondent aux besoins spécifiques de vos cibles.
- **Envoyer des SMS, des WhatsApp ou des e-mails de prospection** : Les numéros de téléphone et adresses e-mail fournis sont utilisés pour envoyer les messages de prospection dans le cadre des campagnes que vous avez commandées.
- **Optimiser la campagne** : Les données peuvent être analysées pour affiner les stratégies de prospection et améliorer l'efficacité de vos campagnes.

4.3. Amélioration de nos services

Nous utilisons les données collectées pour :

- **Comprendre vos besoins** : Les informations que vous nous fournissez nous aident à mieux comprendre vos attentes, ce qui nous permet d'améliorer nos services et d'ajuster nos offres pour répondre au mieux à vos exigences.
- **Analyser les performances** : Les données issues des interactions avec nos services, telles que les réponses aux campagnes de prospection, sont utilisées pour évaluer la performance de nos solutions et les améliorer continuellement.

4.4. Communication d'informations et de promotions

Avec votre consentement, nous pouvons utiliser vos données pour :

- **Vous informer sur nos produits et services** : Nous pouvons vous envoyer des e-mails, des WhatsApp ou des SMS pour vous tenir informé des nouveautés, des offres spéciales, ou des mises à jour de nos services susceptibles de vous intéresser.
- **Envoyer des invitations à des événements** : Si vous avez participé à un événement ou manifesté de l'intérêt pour nos services, nous pouvons vous inviter à des événements futurs ou à des webinaires.

4.5. Gestion de la relation client

Les données personnelles sont également utilisées pour :

- **Assurer un suivi personnalisé** : Nous utilisons vos informations pour gérer notre relation avec vous, en vous offrant un service client réactif et personnalisé.
- **Facturation et administration** : Les données peuvent être utilisées pour gérer les aspects administratifs de notre relation, y compris la facturation, la gestion des contrats, et la comptabilité.

4.6. Respect des obligations légales

Prospectia peut être amenée à utiliser vos données pour :

- **Se conformer aux obligations légales et réglementaires** : Nous pouvons traiter vos données pour respecter nos obligations légales, par exemple en matière de comptabilité, de fiscalité, ou de conservation des données.
- **Répondre aux demandes des autorités compétentes** : En cas de demande légale ou d'enquête, nous pouvons être tenus de communiquer certaines données aux autorités compétentes.

4.7. Sécurité et prévention des fraudes

Nous utilisons également vos données pour :

- **Assurer la sécurité de nos systèmes** : Les données peuvent être utilisées pour détecter, prévenir, et répondre à des activités frauduleuses ou des atteintes à la sécurité de nos systèmes et services.
- **Analyser et prévenir les risques** : Prospectia peut analyser les données pour identifier et atténuer les risques liés à la sécurité des informations.

En utilisant vos données personnelles, Prospectia veille à ce qu'elles soient traitées de manière sécurisée, confidentielle, et en accord avec vos droits et les réglementations en vigueur. Nos pratiques de traitement des données sont conçues pour offrir une valeur ajoutée tout en respectant la confidentialité de vos informations.

5. Partage des données

Prospectia s'engage à protéger la confidentialité de vos données personnelles et à ne les partager qu'avec des tiers dans des circonstances spécifiques et conformément aux réglementations en vigueur. Voici les cas dans lesquels vos données peuvent être partagées :

5.1. Partage avec des sous-traitants

Pour vous fournir nos services, nous faisons appel à des sous-traitants qui agissent pour notre compte et sous notre responsabilité. Ces sous-traitants ont accès à vos données uniquement dans le cadre des tâches qui leur sont confiées et sont tenus de respecter la confidentialité et la sécurité de ces informations. Les principaux sous-traitants sont :

- **Prestataires d'hébergement** : Vos données peuvent être hébergées par des sociétés spécialisées telles que Scaleway (France) ou Contabo (Allemagne), qui garantissent des standards de sécurité élevés. En fonction des besoins et des préférences du client, l'hébergement peut être réalisé sur des serveurs en France, en Allemagne, ou dans d'autres pays respectant les normes de protection des données.
- **Prestataires de services d'inférence** : Pour le traitement de certaines données anonymisées via des moteurs d'inférence, nous pouvons faire appel à des prestataires comme OpenAI (Irlande), Scaleway (France), ou Infomaniak (Suisse). Ces prestataires ne conservent pas vos données personnelles après traitement.

5.2. Partage avec des partenaires commerciaux

Dans certains cas, et avec votre accord explicite, nous pouvons partager vos données avec des partenaires commerciaux pour :

- **Offrir des services complémentaires** : Si vous avez accepté, nous pouvons partager vos données avec des partenaires sélectionnés afin de vous proposer des services ou produits complémentaires susceptibles de vous intéresser.
- **Co-organiser des événements** : Lors de l'organisation d'événements conjointement avec des partenaires, vos données peuvent être partagées pour gérer votre participation et vous fournir des informations pertinentes.

5.3. Partage avec les autorités compétentes

Prospectia peut être amenée à divulguer vos données personnelles aux autorités compétentes dans les cas suivants :

- **Conformité légale** : Si la loi nous oblige à divulguer certaines informations, notamment dans le cadre de procédures judiciaires, fiscales, ou de toute autre obligation légale.
- **Réponse aux demandes des autorités** : Si nous recevons une demande officielle des autorités (police, régulateurs, etc.), nous pouvons être tenus de fournir les données personnelles nécessaires à l'enquête ou à l'action légale.

5.4. Transferts internationaux de données

Lorsque vos données sont transférées en dehors de l'Espace Économique Européen (EEE), nous nous assurons que des garanties adéquates sont en place pour protéger vos données personnelles :

- **Clauses contractuelles types** : Pour les transferts vers des pays n'offrant pas un niveau de protection des données suffisant, nous utilisons des clauses contractuelles types approuvées par la Commission européenne pour garantir la sécurité de vos données.
- **Adhésion à des cadres de protection des données** : Dans certains cas, les transferts peuvent se faire vers des entités adhérant à des cadres de protection des données reconnus, tels que le Privacy Shield (pour les transferts vers les États-Unis, bien que ce cadre soit désormais en révision).

5.5. Partage interne

Vos données peuvent être partagées au sein des équipes internes de Prospectia pour les besoins de la prestation des services. Ces partages sont limités aux collaborateurs qui ont besoin d'accéder à ces informations pour réaliser leurs missions, et ces collaborateurs sont tenus à une stricte obligation de confidentialité.

5.6. Non-partage à des fins commerciales

Prospectia ne vend, ne loue, ni ne partage vos données personnelles avec des tiers à des fins commerciales sans votre consentement explicite. Nous utilisons vos données uniquement pour les finalités pour lesquelles elles ont été collectées et dans le respect de vos droits.

5.7. Sécurité des données partagées

Lorsque nous partageons vos données avec des tiers, nous nous assurons que ces partenaires ou sous-traitants respectent des normes de sécurité rigoureuses pour protéger vos informations contre tout accès non autorisé, perte, ou destruction.

En résumé, Prospectia partage vos données personnelles uniquement dans des cas précis, avec des tiers de confiance, et toujours dans le respect de vos droits et de la législation en vigueur. Nous nous engageons à garantir la sécurité et la confidentialité de vos données à chaque étape de leur traitement.

6. Transfert des données hors de l'Union Européenne

Dans le cadre de la prestation de nos services, il peut être nécessaire pour Prospectia de transférer certaines données personnelles en dehors de l'Espace Économique Européen (EEE). Nous prenons très au sérieux la sécurité et la confidentialité de ces transferts et veillons à ce que vos données bénéficient d'une protection adéquate, conforme aux exigences du Règlement Général sur la Protection des Données (RGPD).

6.1. Transferts nécessaires pour la prestation des services

Dans le cadre de la prestation de nos services, il peut être nécessaire pour Prospectia de transférer certaines données personnelles en dehors de l'Espace Économique Européen (EEE). Nous prenons très au sérieux la sécurité et la confidentialité de ces transferts et veillons à ce que vos données bénéficient d'une protection adéquate, conforme aux exigences du Règlement Général sur la Protection des Données (RGPD).

6.1. Transferts nécessaires pour la prestation des services

Certains de nos prestataires de services, notamment ceux spécialisés dans l'hébergement de données ou les services d'inférence basés sur l'intelligence artificielle, peuvent être situés en dehors de l'EEE. Les principales situations où des transferts de données hors de l'UE peuvent se produire incluent :

- **Utilisation de services cloud** : Par exemple, certains de nos prestataires comme OpenAI, dont les serveurs sont situés en Irlande, peuvent traiter des données anonymisées pour des services d'inférence. Étant donné que l'Irlande est un pays membre de l'Union Européenne, ces transferts sont conformes aux standards de sécurité les plus stricts sans nécessiter de garanties supplémentaires.
- **Hébergement de données** : Dans certains cas, les données peuvent être hébergées sur des serveurs situés en dehors de l'EEE, par exemple chez Infomaniak (Suisse), une société située dans un pays offrant un niveau de protection des données reconnu comme adéquat par la Commission européenne.

6.2. Garanties de protection des données

Pour chaque transfert de données en dehors de l'EEE, Prospectia met en place des garanties appropriées pour assurer la protection de vos informations personnelles :

- **Clauses contractuelles types (CCT)** : Pour les transferts vers des pays qui ne bénéficient pas d'une décision d'adéquation de la Commission européenne, nous utilisons des Clauses Contractuelles Types approuvées par la Commission. Ces clauses standardisées imposent aux parties contractantes de respecter les standards de protection des données équivalents à ceux de l'UE.
- **Décisions d'adéquation** : Lorsque les données sont transférées vers un pays ayant reçu une décision d'adéquation de la Commission européenne (comme la Suisse), nous procédons aux transferts sans nécessiter de garanties supplémentaires, car ces pays sont réputés offrir un niveau de protection des données comparable à celui de l'UE.
- **Transferts intra-UE** : Les transferts de données vers OpenAI en Irlande sont effectués au sein de l'Union Européenne, ce qui signifie qu'ils sont soumis aux mêmes règles et protections strictes que les transferts effectués au sein de tout autre État membre de l'UE.

6.3. Transparence et information

Prospectia s'engage à vous informer de manière transparente sur les transferts de vos données personnelles en dehors de l'EEE. Si vous souhaitez en savoir plus sur les mesures de protection mises en place ou obtenir une copie des clauses contractuelles types ou autres garanties applicables, vous pouvez contacter notre Délégué à la Protection des Données (DPO) aux coordonnées fournies.

6.4. Sécurité des transferts

Nous prenons toutes les précautions nécessaires pour garantir que les données transférées bénéficient d'un niveau de protection adéquat, y compris en matière de sécurité. Cela inclut des mesures techniques et organisationnelles robustes pour prévenir toute perte, accès non autorisé, ou divulgation des données lors de leur transfert.

6.5. Droits des personnes concernées

Vos droits concernant vos données personnelles, tels que le droit d'accès, de rectification, d'effacement, et d'opposition, restent applicables même lorsque vos données sont transférées en dehors de l'EEE. Vous pouvez exercer ces droits à tout moment en contactant notre DPO.

6.6. Réévaluation des transferts

Prospectia réévalue régulièrement les transferts de données et les garanties associées pour s'assurer qu'ils continuent de respecter les exigences du RGPD et de protéger vos données personnelles de manière adéquate.

En concluant des accords conformes au RGPD avec nos prestataires et en appliquant des mesures de protection rigoureuses, Prospectia veille à ce que vos données personnelles soient protégées même lorsqu'elles sont transférées en dehors de l'Union Européenne.

7. Conservation des données

Prospectia s'engage à conserver vos données personnelles uniquement pendant la durée nécessaire aux finalités pour lesquelles elles ont été collectées, conformément aux exigences légales et réglementaires. Voici les détails sur notre politique de conservation des données :

7.1. Durée de conservation en fonction des finalités

- **Données de contact et de gestion des clients** : Les données collectées via les formulaires de contact, les demandes de devis, ou lors d'événements sont conservées pendant toute la durée de la relation commerciale. Après la fin de cette relation, ces données sont archivées pour une durée de 3 ans, à des fins de gestion des relations clients, sauf obligation légale de les conserver plus longtemps.
- **Données de prospection** : Les données personnelles utilisées pour les campagnes de prospection sont conservées pendant la durée de la campagne, puis archivées pour une durée maximale de 3 ans après la dernière interaction avec le prospect, conformément aux recommandations de la CNIL, sauf obligation légale contraire.
- **Données de facturation et transactions commerciales** : Les données liées à la facturation, aux paiements, et aux transactions commerciales sont conservées pendant une durée de 10 ans à compter de la clôture de l'exercice comptable, en conformité avec les obligations fiscales et comptables en vigueur.
- **Données liées aux événements** : Les informations collectées lors de votre participation à des événements sont conservées pendant une durée de 3 ans à compter de la dernière interaction avec Prospectia, à des fins de gestion des relations et d'organisation d'événements futurs.
- **Données de navigation** : Les données de navigation collectées via les cookies sont conservées pendant une durée maximale de 13 mois. Après ce délai, elles sont soit supprimées, soit anonymisées pour des analyses statistiques.

7.2. Archivage des données

Après la fin des périodes de conservation actives, certaines données peuvent être archivées avec un accès restreint pour répondre à des obligations légales, gérer des contentieux éventuels, ou répondre aux demandes des autorités compétentes. Les données archivées sont conservées pendant la durée nécessaire pour respecter ces obligations.

7.3. Suppression des données

À l'issue de la période de conservation ou d'archivage, vos données personnelles sont supprimées de manière sécurisée. Si vous exercez votre droit à l'effacement avant la fin de la période de conservation, nous procéderons à la suppression de vos données, sauf si leur conservation est requise par la loi (par exemple, pour des raisons fiscales ou de sécurité).

7.4. Conservation des données anonymisées

Certaines données peuvent être anonymisées après la fin de la période de conservation active. Ces données anonymisées, qui ne permettent plus de vous identifier directement, peuvent être conservées indéfiniment à des fins de recherche, de statistiques, ou d'amélioration des services de Prospectia.

7.5. Droits des personnes concernées

Vous avez le droit de demander des informations sur la durée de conservation de vos données personnelles, ainsi que le droit de demander leur suppression ou leur anonymisation avant l'expiration de la période de conservation, sous réserve des obligations légales de Prospectia.

7.6. Sécurité des données conservées

Pendant toute la durée de conservation, Prospectia met en place des mesures de sécurité techniques et organisationnelles pour protéger vos données contre tout accès non autorisé, altération, perte ou destruction.
En définissant clairement les durées de conservation des données en fonction de leur utilisation et en garantissant leur suppression sécurisée après expiration, Prospectia s'assure de respecter vos droits tout en se conformant aux obligations légales applicables.

8. Vos droits

Conformément au Règlement Général sur la Protection des Données (RGPD) et à la législation française en vigueur, vous disposez de plusieurs droits concernant vos données personnelles. Prospectia s'engage à respecter ces droits et à faciliter leur exercice. Voici les détails des droits dont vous bénéficiez :

8.1. Droit d'accès

Vous avez le droit de demander à Prospectia la confirmation que des données personnelles vous concernant sont traitées, ainsi que d'accéder à ces données. Vous pouvez également obtenir des informations sur les finalités du traitement, les catégories de données concernées, les destinataires de vos données, et la durée de conservation.

8.2. Droit de rectification

Si vous constatez que les données personnelles détenues par Prospectia sont inexactes ou incomplètes, vous avez le droit de demander leur rectification. Prospectia s'engage à corriger ou compléter les données dans les plus brefs délais.

8.3. Droit à l'effacement (droit à l'oubli)

Vous pouvez demander l'effacement de vos données personnelles dans les cas suivants :

- Les données ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées.
- Vous retirez votre consentement (si le traitement était basé sur le consentement).
- Vous vous opposez au traitement et il n'existe pas de motif légitime impérieux pour poursuivre le traitement.
- Les données ont été traitées illégalement.
- Les données doivent être effacées pour respecter une obligation légale.

Prospectia examinera votre demande et, sous réserve des obligations légales de conservation, procédera à l'effacement des données concernées.

8.4. Droit à la limitation du traitement

Vous avez le droit de demander la limitation du traitement de vos données personnelles dans les circonstances suivantes :

- Vous contestez l'exactitude des données (pendant la vérification de leur exactitude par Prospectia).
- Le traitement est illégal mais vous vous opposez à l'effacement des données et demandez plutôt la limitation de leur utilisation.
- Prospectia n'a plus besoin des données, mais vous en avez besoin pour la constatation, l'exercice ou la défense de droits en justice.
- Vous vous êtes opposé au traitement et une vérification est en cours pour déterminer si les motifs légitimes de Prospectia prévalent.

8.5. Droit à la portabilité des données

Vous avez le droit de recevoir les données personnelles que vous avez fournies à Prospectia dans un format structuré, couramment utilisé et lisible par machine, et de les transmettre à un autre responsable de traitement. Ce droit s'applique lorsque :

- Le traitement est fondé sur votre consentement ou sur un contrat.
- Le traitement est effectué à l'aide de procédés automatisés.

Vous pouvez également demander que vos données soient directement transférées à un autre responsable de traitement, lorsque cela est techniquement possible.

8.6. Droit d'opposition

Vous pouvez vous opposer à tout moment, pour des raisons tenant à votre situation particulière, au traitement de vos données personnelles basé sur l'intérêt légitime de Prospectia. Prospectia cessera alors de traiter vos données, sauf s'il existe des motifs légitimes impérieux pour le traitement qui prévalent sur vos intérêts et droits, ou pour la constatation, l'exercice ou la défense de droits en justice. Vous pouvez également vous opposer à tout moment au traitement de vos données à des fins de prospection commerciale.

8.7. Droit de retirer votre consentement

Lorsque le traitement de vos données personnelles est basé sur votre consentement, vous avez le droit de retirer ce consentement à tout moment. Le retrait de votre consentement ne remet pas en cause la licéité du traitement effectué avant ce retrait.

8.8. Droit de définir des directives post-mortem

Vous avez le droit de définir des directives concernant la conservation, l'effacement et la communication de vos données personnelles après votre décès. Ces directives peuvent être générales ou spécifiques. Prospectia respectera ces directives, sauf si la loi en dispose autrement.

8.9. Exercice de vos droits

Pour exercer vos droits, vous pouvez contacter le Délégué à la Protection des Données (DPO) de Prospectia :

- **Nom** : Enzo Blanchon
- **E-mail** : blanchonenzo@gmail.com
- **Adresse** : 1 Rue Traversière, 31450 Baziège
- **Téléphone** : 06 25 81 18 10

Prospectia s'engage à répondre à votre demande dans un délai d'un mois. Ce délai peut être prolongé de deux mois en fonction de la complexité et du nombre de demandes, auquel cas vous en serez informé.

8.10. Droit d'introduire une réclamation auprès d'une autorité de contrôle

Si vous estimez que Prospectia ne respecte pas ses obligations au regard de vos données personnelles, vous avez le droit d'introduire une réclamation auprès de l'autorité de contrôle compétente, en France, la Commission Nationale de l'Informatique et des Libertés (CNIL) :

- **Site web** : www.cnil.fr
- **Adresse** : 3 Place de Fontenoy, TSA 80715, 75334 Paris Cedex 07

En exerçant vos droits, vous contribuez à la protection de vos données personnelles et à leur traitement conforme à la réglementation en vigueur. Prospectia est à votre disposition pour vous assister dans l'exercice de ces droits et pour garantir la transparence et la sécurité de vos informations personnelles.

9. Sécurité des données

La sécurité de vos données personnelles est une priorité pour Prospectia. Nous mettons en œuvre des mesures techniques et organisationnelles robustes pour protéger vos informations contre toute perte, altération, divulgation ou accès non autorisé. Voici comment nous assurons la sécurité de vos données :

9.1. Mesures techniques de sécurité

- **Chiffrement des données** : Toutes les données personnelles traitées par Prospectia sont chiffrées, à la fois lors de leur transmission et de leur stockage, afin de protéger vos informations contre les accès non autorisés. Cela inclut le chiffrement des données stockées sur nos serveurs ainsi que celles transmises via Internet.
- **Contrôles d'accès** : L'accès aux données personnelles est strictement limité aux employés et prestataires de services autorisés qui ont besoin de ces informations pour accomplir leurs tâches. Chaque utilisateur dispose de droits d'accès définis en fonction de son rôle, ce qui réduit les risques de fuite ou d'utilisation abusive des données.
- **Pare-feu et systèmes de détection d'intrusion** : Prospectia utilise des pare-feu de pointe et des systèmes de détection d'intrusion pour protéger ses systèmes informatiques contre les attaques externes. Ces technologies permettent de surveiller et d'empêcher les tentatives d'accès non autorisées à nos systèmes.
- **Sauvegardes régulières** : Des sauvegardes régulières des données sont effectuées pour assurer leur intégrité et permettre une restauration rapide en cas d'incident. Ces sauvegardes sont également chiffrées et stockées de manière sécurisée.

9.2. Mesures organisationnelles de sécurité

- **Politique de sécurité des informations** : Prospectia a mis en place une politique de sécurité des informations qui définit les procédures et les bonnes pratiques à suivre pour protéger les données personnelles. Cette politique est régulièrement mise à jour pour s'adapter aux nouvelles menaces et aux évolutions technologiques.
- **Formation des employés** : Tous les employés de Prospectia sont formés aux meilleures pratiques en matière de sécurité des données. Des sessions de sensibilisation régulières sont organisées pour garantir que chacun est conscient des enjeux de la sécurité des informations et des procédures à suivre.
- **Confidentialité contractuelle** : Tous les employés et sous-traitants de Prospectia sont tenus de signer des accords de confidentialité. Ces accords garantissent que les données personnelles auxquelles ils ont accès sont traitées avec le plus grand respect et conformément aux exigences légales.
- **Gestion des incidents de sécurité** : Prospectia dispose d'une procédure de gestion des incidents de sécurité qui prévoit des actions immédiates en cas de violation des données. Cela inclut la notification rapide des personnes concernées et, le cas échéant, de l'autorité de contrôle compétente.

9.3. Audit et surveillance

- **Audits réguliers** : Prospectia réalise régulièrement des audits de sécurité pour identifier les vulnérabilités potentielles et mettre en œuvre les améliorations nécessaires. Ces audits sont effectués par des experts internes ou des tiers indépendants.
- **Surveillance continue** : Nos systèmes de sécurité sont surveillés en permanence pour détecter les activités suspectes ou les tentatives d'intrusion. Toute anomalie est immédiatement analysée et traitée pour prévenir tout impact sur la sécurité des données.

9.4. Sécurisation des sous-traitants

- **Engagements contractuels** : Prospectia impose à ses sous-traitants des obligations strictes en matière de sécurité des données. Nous nous assurons que nos sous-traitants respectent les mêmes standards de sécurité que ceux appliqués en interne, via des clauses contractuelles spécifiques.
- **Évaluation des sous-traitants** : Avant de travailler avec un sous-traitant, Prospectia évalue ses pratiques de sécurité pour s'assurer qu'elles répondent à nos exigences. Cette évaluation est renouvelée périodiquement pour vérifier la conformité continue du sous-traitant.

9.5. Sécurité des données transférées

- **Transferts sécurisés** : Lors du transfert de données personnelles, que ce soit au sein de l'Union Européenne ou en dehors, Prospectia s'assure que des protocoles de sécurité adaptés sont en place, comme le chiffrement des données pendant leur transmission.
- **Clauses de protection** : Pour les transferts de données vers des pays hors de l'EEE, Prospectia utilise des clauses contractuelles types approuvées par la Commission européenne ou d'autres mécanismes de protection reconnus pour garantir la sécurité et la confidentialité des données transférées.

9.6. Sécurité des données physiques

- **Protection des installations** : Les locaux de Prospectia et les centres de données où sont hébergées vos données sont protégés par des systèmes de sécurité physique, incluant la surveillance par vidéo, le contrôle d'accès biométrique, et des systèmes d'alarme.
- **Accès restreint** : L'accès aux installations où sont stockées les données est strictement contrôlé et réservé aux personnes autorisées. Seuls les personnels habilités ont accès aux serveurs et aux dispositifs de stockage contenant des données personnelles.

En mettant en œuvre ces mesures de sécurité rigoureuses, Prospectia s'engage à protéger vos données personnelles contre toute menace et à assurer leur confidentialité, intégrité et disponibilité à tout moment. Nous révisons régulièrement nos pratiques de sécurité pour rester à la pointe de la protection des données et garantir un niveau de sécurité optimal.

10. Modifications de la politique de confidentialité

Prospectia se réserve le droit de modifier la présente politique de confidentialité à tout moment, afin de refléter les évolutions législatives, réglementaires, ou les changements dans nos pratiques de traitement des données. Voici comment nous procédons pour informer nos clients de ces modifications :

10.1. Notification des modifications

Lorsque nous apportons des modifications significatives à notre politique de confidentialité, nous nous engageons à vous en informer de manière transparente. Cela peut inclure :

- **Notification par e-mail** : Si vous êtes un client enregistré, nous vous enverrons un e-mail pour vous informer des modifications apportées à la politique de confidentialité.
- **Mise à jour sur notre site web** : Nous publierons la version mise à jour de la politique de confidentialité sur notre site internet, avec une indication claire de la date de la dernière révision. La nouvelle version de la politique sera accessible à tout moment.

10.2. Prise d'effet des modifications

Les modifications apportées à la politique de confidentialité prendront effet immédiatement après leur publication sur notre site internet, sauf mention contraire dans la notification. En continuant à utiliser nos services après l'entrée en vigueur des modifications, vous acceptez les termes de la nouvelle politique de confidentialité.

10.3. Consultation régulière

Nous encourageons nos clients à consulter régulièrement la politique de confidentialité pour rester informés des éventuelles modifications. La date de la dernière mise à jour sera toujours indiquée en haut de la politique, afin que vous puissiez identifier rapidement les changements récents.

10.4. Droits en cas de modification

Si vous n'acceptez pas les modifications apportées à la politique de confidentialité, vous avez le droit de demander l'arrêt du traitement de vos données personnelles en contactant notre Délégué à la Protection des Données (DPO). Vous pouvez également exercer vos droits, tels que le droit à l'effacement, conformément aux procédures décrites dans cette politique.

10.5. Modifications mineures

Certaines modifications mineures, qui n'affectent pas de manière substantielle vos droits ou les obligations de Prospectia, peuvent être apportées sans notification préalable. Toutefois, ces modifications seront également indiquées sur notre site internet.
En assurant une communication claire et transparente sur les modifications de la politique de confidentialité, Prospectia s'engage à maintenir la confiance de ses clients et à respecter leurs droits en matière de protection des données personnelles.

11. Contact et réclamations

Prospectia s'engage à être disponible pour répondre à toutes vos questions, préoccupations, ou réclamations concernant la protection de vos données personnelles. Voici comment vous pouvez nous contacter et quelles sont vos options en cas de réclamation.

11.1. Contact pour les questions sur la politique de confidentialité

Si vous avez des questions concernant cette politique de confidentialité, ou si vous souhaitez exercer vos droits relatifs à vos données personnelles, vous pouvez contacter notre Délégué à la Protection des Données (DPO) :

- **Nom** : Enzo Blanchon
- **Adresse** : 1 Rue Traversière, 31450 Baziège
- **E-mail** : blanchonenzo@gmail.com
- **Téléphone** : 06 25 81 18 10

Nous nous engageons à répondre à vos demandes dans un délai raisonnable, et en tout état de cause, dans les délais prescrits par la loi (généralement un mois).

11.2. Réclamations

Si vous estimez que Prospectia ne respecte pas ses obligations légales en matière de protection des données ou si vous n'êtes pas satisfait de la réponse apportée à une de vos demandes, vous avez plusieurs options pour déposer une réclamation :

- **Réclamation auprès de Prospectia** : Vous pouvez adresser une réclamation directement à notre DPO en utilisant les coordonnées mentionnées ci-dessus. Nous traiterons votre réclamation avec sérieux et veillerons à y apporter une réponse dans les meilleurs délais.
- **Réclamation auprès de l'autorité de contrôle** : Si vous n'êtes pas satisfait de la réponse de Prospectia ou si vous pensez que vos droits n'ont pas été respectés, vous pouvez déposer une réclamation auprès de l'autorité de contrôle compétente. En France, l'autorité de contrôle est la Commission Nationale de l'Informatique et des Libertés (CNIL) :
    - **Site web** : www.cnil.fr
    - **Adresse** : 3 Place de Fontenoy, TSA 80715, 75334 Paris Cedex 07
    - **Téléphone** : 01 53 73 22 22

11.3. Démarches préalables

Avant de déposer une réclamation auprès de la CNIL ou de toute autre autorité compétente, nous vous invitons à nous contacter directement pour essayer de résoudre votre problème de manière amiable. Nous nous engageons à faire tout notre possible pour répondre à vos préoccupations et trouver une solution satisfaisante.

11.4. Informations complémentaires

Pour toute autre information relative à vos droits ou à la protection de vos données personnelles, vous pouvez également consulter le site internet de la CNIL, qui offre des ressources et des conseils utiles pour les individus souhaitant mieux comprendre leurs droits.

En mettant à disposition ces points de contact et en assurant une réponse rapide à vos demandes, Prospectia vise à garantir la transparence et le respect de vos droits en matière de protection des données personnelles. Nous sommes déterminés à traiter chaque demande avec le plus grand soin et à maintenir la confiance que vous nous accordez.

Annexe 2 : Prospectia - Registre simplifié des traitements

Prospectia - Registre Simplifié des Traitements

Dernière mise à jour : 14 août 2024

Conformément au Règlement Général sur la Protection des Données (RGPD), Prospectia tient un registre des traitements simplifié pour assurer la transparence et la conformité dans le traitement des données personnelles. Ce registre documente les principales activités de traitement des données personnelles effectuées par notre société.

1. Coordonnées du Responsable de Traitement

- **Nom** : Thomas Peyre
- **Fonction** : Président de Prospectia
- **Adresse** : 1 Rue Traversière, 31450 Baziège, France
- **Téléphone** : 06 25 81 18 10
- **E-mail** : peyrethomas@gmail.com

2. Coordonnées du Délégué à la Protection des Données (DPO)

- **Nom** : Enzo Blanchon
- **Fonction** : Délégué à la Protection des Données
- **Adresse** : 1 Rue Traversière, 31450 Baziège, France
- **Téléphone** : 06 25 81 18 10
- **E-mail** : blanchonenzo@gmail.com

3. Finalités des traitements

Nom du traitement	Référence	Date de création	Dernière mise à jour	Finalité du traitement	Données sensibles ?
Entraînement de l'IA	0001	01/01/2023	01/05/2024	Fine tuning d'un modèle IA	Non
Inférence	0002	01/01/2023	01/05/2024	Génération des messages	Non
Post-traitement	0003	01/01/2023	01/05/2024	Détection et correction d'erreurs	Non

4. Catégories de données collectées

1. **Données de contact** : Nom, prénom, adresse e-mail, numéro de téléphone.
2. **Données de transaction** : Informations de paiement, adresse postale pour la facturation.
3. **Données de prospection** : Informations fournies par le client, y compris noms, prénoms, numéros de téléphone, et adresses e-mail des prospects.
4. **Données techniques** : Adresse IP, cookies, données de navigation.
5. **Données liées aux campagnes** : Contenus des messages, réponses des prospects, taux de conversion.

5. Catégories de personnes concernées

1. **Clients de Prospectia** : Personnes physiques ou morales ayant souscrit aux services de Prospectia.
2. **Prospects** : Personnes physiques ou morales ciblées par les campagnes de prospection menées par Prospectia pour le compte de ses clients.
3. **Participants à des événements** : Personnes ayant participé à des événements organisés ou sponsorisés par Prospectia.
4. **Utilisateurs du site web** : Visiteurs du site internet de Prospectia.

6. Destinataires des données

1. **Sous-traitants** : Hébergeurs de données (Scaleway, Contabo), services d'inférence (OpenAI, Infomaniak).
2. **Partenaires commerciaux** : Partenaires ayant un lien direct avec les services fournis (avec consentement explicite du client).
3. **Autorités compétentes** : En cas de demande légale, les données peuvent être partagées avec les autorités compétentes (police, CNIL, etc.).

7. Transferts internationaux de données

- **Hébergeurs** : Scaleway (France), Contabo (Allemagne), Infomaniak (Suisse).
- **Services d'inférence** : OpenAI (Irlande), Infomaniak (Suisse).
- Les transferts de données en dehors de l'Union Européenne sont encadrés par des clauses contractuelles types et d'autres mécanismes de protection reconnus par le RGPD.

8. Durée de conservation des données

1. **Données de contact** : Conservées pendant la durée de la relation commerciale, puis archivées pendant 3 ans.
2. **Données de transaction** : Conservées pendant 10 ans à des fins comptables et fiscales.
3. **Données de prospection** : Conservées pendant 3 ans après la dernière interaction avec le prospect.
4. **Données techniques** : Conservées pendant 13 mois pour les cookies.

9. Sécurité des traitements

Prospectia applique des mesures de sécurité techniques et organisationnelles strictes pour protéger les données personnelles, notamment :

- **Chiffrement des données**
- **Contrôles d'accès**
- **Pare-feu et systèmes de détection d'intrusion**
- **Audits de sécurité réguliers**

10. Droits des personnes concernées

Les personnes concernées par les traitements effectués par Prospectia disposent des droits suivants :

- Droit d'accès, de rectification, d'effacement, de limitation du traitement, de portabilité, et d'opposition.
- Droit de retirer leur consentement à tout moment pour les traitements fondés sur le consentement.
- Droit de déposer une réclamation auprès de la CNIL.

Pour exercer ces droits, les personnes concernées peuvent contacter le DPO aux coordonnées mentionnées ci-dessus.

Ce registre simplifié des traitements reflète l'engagement de Prospectia à assurer la transparence et la conformité dans le traitement des données personnelles conformément aux exigences du RGPD.

Annexe 3 : Data Processing Agreement (DPA) de Scaleway

ACCORD DE SOUS-TRAITANCE DU TRAITEMENT DE DONNEES A CARACTERE PERSONNEL

Le présent Accord de Sous-traitance fait partie intégrante du contrat portant sur des prestations de Service de Scaleway conclu entre le Client et Scaleway (« **Contrat** »), lorsque Scaleway exécute des Traitements de Données à Caractère Personnel pour le compte du Client en qualité de Sous-Traitant au sens du RGPD.

Aux fins de la réalisation et de l'exécution du Contrat, des Données à Caractère Personnel au sens du Règlement (UE) 2016/679 du Parlement européen et du Conseil 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 (« **RGPD** ») pourront être communiquées à Scaleway et/ou celle-ci pourra y avoir accès.

Le présent Accord de sous-traitance a pour objet de définir les conditions dans lesquelles Scaleway s'engage à effectuer, aux seules fins de la stricte exécution du Contrat, pour le compte du Client et pendant la seule durée du Contrat, les opérations de Traitement des Données à Caractère Personnel. Les Parties s'engagent dès à présent à respecter la Réglementation relative à la Protection des Données.

Le présent Accord est applicable aux prestations objets du Contrat pour lesquelles le Client agit en qualité de responsable du traitement au sens du RGPD, en ce qui concerne les Données à Caractère Personnel et Scaleway agit en qualité de sous-traitant au sens du RGPD.

Le Client s'est assuré, sur la base des informations fournies par Scaleway et des autres informations à sa disposition, que Scaleway présente des garanties suffisantes, notamment en termes d'expérience, de ressources, de capacités et de fiabilité, afin de mettre en œuvre les mesures techniques et organisationnelles nécessaires pour que le Traitement des Données à Caractère Personnel prévu par le Contrat soit effectué de manière conforme à la Réglementation relative à la Protection des Données.

Article 1 - Définitions

En sus des termes et expressions définis dans le présent Accord de Sous-traitance (« **Accord de Sous-traitance** »), les termes et expressions « **Organisation Internationale** », « **Délégué à la Protection des Données** » et « **Violation des Données à Caractère Personnel** » ont la même signification que celle qui leur est attribuée dans le RGPD. En outre, les termes et expressions suivants ont la signification indiquée ci-après, qu'ils soient employés au singulier ou au pluriel :

« **Données à Caractère Personnel** » désigne toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale qui pourront être communiquées ou mises à disposition dans le cadre de la réalisation et l'exécution du Contrat ;

« **Mesures de Sécurité** » désigne les mesures de sécurité prévues par la Réglementation relative à la Protection des Données ainsi que toute autre obligation prévue par ladite Réglementation afin de garantir la sécurité et la confidentialité des Données à Caractère Personnel, y compris les activités devant être exécutées en cas de Violation des Données à Caractère Personnel, notamment afin d'éviter ou de réduire les effets néfastes de la Violation des Données à Caractère Personnel sur les Personnes Concernées ;

« **Préposé** » désigne les salariés, personnes mandatées ou toute autre personne physique habilitée à exécuter des opérations de Traitement des Données à Caractère Personnel communiquées ou mises à disposition par Scaleway et/ou ses éventuels Sous-traitants Ultérieurs ;

« **Personne Concernée** » désigne, conformément au RGPD, les personnes physiques identifiées ou identifiables auxquelles les Données à Caractère Personnel font référence;

« **Réglementation relative à la Protection des Données** » désigne le RGPD, la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et ses évolutions successives (« **Loi Informatique et Libertés** »), la Directive 2002/58/CE du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électronique du 12 juillet 2002, ainsi que l'ensemble des dispositions législatives, réglementations, lignes directrices, opinions, certifications, agréments, recommandations ou décisions de justice définitives relative à la protection des données à caractère personnel applicable au Traitement des Données à Caractère Personnel, déjà en vigueur ou qui entrera en vigueur pendant la durée du présent Accord de Sous-traitance, et de toute autre autorité compétente. En cas de contradiction entre la Loi Informatique et Libertés, le RGPD et/ou les mesures adoptées par les autorités compétentes dans la mise en œuvre de ceux-ci, les dispositions du RGPD et les mesures adoptées aux fins de sa mise en œuvre prévaudront.

« **Traitement(s)** » désigne le ou les traitements de Données à Caractère Personnel au sens du RGPD, confié(s) à Scaleway dans le cadre du Contrat et décrit(s) au présent Accord de Sous-traitance.

Article 2 - Traitement(s) faisant l'objet de la Sous-Traitance

2.1 Le Traitement effectué par Scaleway aux fins du présent Accord de Sous-traitance portera uniquement sur les types de Données à Caractère Personnel et les

catégories de Personnes Concernées définies par le Client et sous sa responsabilité.

2.2 Il est précisé que les Services du Sous-traitant ne permettent pas le traitement de données de santé à caractère personnel conformément à la certification imposée par la loi (articles L.1111-8 et suivants du code de la santé publique). En conséquence le Client s'engage à ne traiter aucune donnée de santé à caractère personnel par l'intermédiaire des services du Sous-traitant.

2.3 Le Client s'engage à fournir au Sous-Traitant les données visées au présent Accord de Sous-traitance pour les besoins de l'exécution du Contrat et à documenter par écrit toute instruction concernant le Traitement des Données à Caractère Personnel par le Sous-Traitant.

2.4 Scaleway s'engage à garantir la confidentialité des Données à Caractère Personnel et à ce que tous Préposés et Sous-traitants Ultérieurs autorisés à traiter les Données à Caractère Personnel en vertu du présent Accord de Sous-traitance, respectent la confidentialité des Données à Caractère Personnel. L'obligation de confidentialité des Données à Caractère Personnel restera en vigueur cinq ans à compter de l'expiration du Contrat.

Article 3 - Nature, finalités et modalités du Traitement

3.1 Scaleway, en qualité de Sous-Traitant du Traitement, s'engage, à ses frais, à :

a) traiter les Données à Caractère Personnel dans le but d'exécuter le Contrat dans les limites et selon les modalités stipulées dans celui-ci, le présent Accord de Sous-traitance et la Réglementation relative à la Protection des Données ;

b) respecter les instructions écrites communiquées par le Client et à informer ce dernier si elle considère qu'une instruction enfreint la Réglementation relative à la Protection des Données ou, plus généralement, la législation applicable ;

c) traiter les Données à Caractère Personnel qui sont strictement nécessaires à l'exécution du Contrat ou au respect des obligations légales ;

d) traiter les Données à Caractère Personnel de manière licite, et conformément au Contrat, au présent Accord de Sous-traitance et aux exigences fixées par la Réglementation relative à la Protection des Données ;

e) signaler, dans la mesure du possible, au Client les éventuelles exigences de modification, de mise à jour, de correction ou de suppression des Données à Caractère Personnel et s'engager à mettre à jour, à modifier, à corriger ou à supprimer à la demande du Client ;

f) assister le Client et collaborer avec lui en cas de demande formulée par les autorités compétentes ou des Personnes Concernées et afin de se conformer aux obligations nées de la Réglementation relative à la Protection des Données ;

g) mettre à la disposition du Client toutes les informations en sa possession, nécessaires, dans le cadre de l'exécution du Contrat, afin de démontrer que celle-ci respecte les obligations visées par la Réglementation relative à la Protection des Données.

Article 4 - Registre des activités relatives au Traitement

4.1 Scaleway s'engage à tenir un registre concernant toutes les catégories d'activités relatives au Traitement des Données à Caractère Personnel effectuées pour le compte du Client. Celui-ci comportera :

a) le nom et les coordonnées de Scaleway et de ses Sous-traitants Ultérieurs, ceux du Client et, le cas échéant, du Délégué à la Protection des Données du Client et de Scaleway ;

b) les catégories des Traitements effectués pour le compte du Client ;

c) le cas échéant, les transferts de Données à Caractère Personnel vers un pays tiers ou à une Organisation Internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, du RGPD, les documents attestant de l'existence des garanties appropriées imposées par l'article 49 du RGPD ; et

d) une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1, du RGPD. Ces mesures de sécurité figurent également dans la Politique de Sécurité des Systèmes d'Information (PSSI) de Scaleway, figurant sur son site web.

4.2 Scaleway s'engage à fournir dans les meilleurs délais au Client une copie du registre visé à la clause 4.1 à la demande de celui-ci et/ou des autorités compétentes.

4.3 Scaleway s'engage à fournir au Client toutes les informations relatives aux Traitements des Données à Caractère Personnel le concernant, dans le cadre de l'exécution du Contrat, dont celui-ci a raisonnablement besoin afin de pouvoir établir son propre registre des activités, relatives aux traitements visés à l'article 30, paragraphe 1, du RGPD.

Article 5 - Obligations du Client Responsable de Traitement

5.1 Le Client est seul responsable des Données à Caractère Personnel et de leur contenu qui transitent par les Services du Sous-traitant. Le Sous-traitant ne peut assurer aucune vérification du contenu des données et ne saurait être responsable de leur éventuel caractère illégal ou illicite, ce que le Client reconnaît expressément.

5.2 Tout(e) collecte, traitement, transmission, diffusion ou représentation d'informations ou données via les Services par le Client, en sa qualité de Responsable du Traitement, sont effectués sous sa seule et entière responsabilité et dans le strict respect de la Réglementation relative à la Protection des Données Applicable.

5.3 Le Client s'engage notamment à :

a) Fournir l'information aux Personnes Concernées par les opérations de traitement au moment de la collecte des données ;

b) Fournir au Sous-traitant les instructions de traitement des Données à Caractère Personnel ;

c) Tenir un registre des activités de traitement mentionnant le Sous-Traitant pour les activités de traitement concernées ;

d) Procéder ou faire procéder sous sa responsabilité aux analyses d'impact, le cas échéant, consulter l'autorité de contrôle compétente, lorsque le traitement envisagé sera susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées ;

e) Fixer la durée de conservation, les modalités d'archivages et d'effacement des Données à Caractère Personnel traitées ;

f) Déterminer et respecter les mesures techniques et organisationnelles relatives à la protection, la sécurité et la confidentialité des Données à Caractère Personnel traitées, mettre en place une procédure interne afin d'identifier et traiter les violations des Données à Caractère Personnel nécessitant une notification à l'autorité de contrôle compétente et/ou aux personnes concernées ;

g) Ne pas traiter de données de santé dans le cadre de l'exécution du Contrat.

Article 6 - Obligations relatives aux Préposés

6.1 Scaleway s'engage à faire en sorte que les Préposés aient exclusivement accès aux Données à Caractère Personnel qui sont strictement nécessaires à l'exécution du Contrat ou afin d'exécuter les obligations légales et Traitent exclusivement ces

Données à Caractère Personnel, dans tous les cas, dans les limites et les termes du présent Accord de Sous-traitance, du Contrat et de la Réglementation relative à la Protection des Données.

6.2 Scaleway s'engage également à n'autoriser le Traitement des Données à Caractère Personnel qu'aux Préposés qui :

a) de par leur expérience, leurs capacités et leur formation s'avèrent aptes à garantir le respect de la Réglementation relative à la Protection des Données et qui doivent y accéder afin d'exécuter le Contrat ;

b) doivent respecter des obligations de confidentialité strictes pendant le Traitement des Données à Caractère Personnel et veiller à la bonne exécution, par les Préposés, des instructions reçues ainsi que des obligations leur incombant.

6.3 Scaleway s'engage, dans le périmètre des services, à établir des mesures physiques, techniques et organisationnelles destinées à faire en sorte que :

a) chaque Préposé puisse avoir accès exclusivement aux Données à Caractère Personnel pouvant faire l'objet d'un Traitement en fonction de l'autorisation dont ce Préposé dispose ;

b) les éventuels Traitements de Données à Caractère Personnel constituant un manquement au regard du présent Accord de Sous-Traitance, du Contrat et/ou de la Réglementation relative à la Protection des Données soient sans délai identifiés et signalés au Client, y compris selon la procédure et dans les délais visés à l'Article 8 en cas de Violation des Données à Caractère Personnel ; et

c) à l'extinction du Contrat ou de la mission confiée au Préposé, le Préposé cesse immédiatement le Traitement des Données à Caractère Personnel, dans le respect des contraintes légales lui incombant.

Article 7 - Sous-traitants Ultérieurs

7.1 Le Client accorde au Sous-traitant une autorisation générale de sous-traitance d'une partie de ses obligations au titre du présent Accord à un autre sous-traitant. Scaleway ne pourra faire appel à un autre sous-traitant (« **Sous-traitant Ultérieur** ») que pour mener des activités de Traitement spécifiques.

7.2 Dans l'hypothèse où Scaleway a recours à un Sous-traitant Ultérieur, Scaleway veillera à ce que chaque Sous-traitant Ultérieur présente des garanties adéquates au regard de la Réglementation relative à la Protection des Données eu égard aux mesures techniques et organisationnelles adoptées pour le Traitement des Données à Caractère Personnel et s'assure que chaque Sous-traitant Ultérieur cesse

immédiatement le Traitement des Données à Caractère Personnel si ces garanties viennent à faire défaut. Si un Sous-traitant Ultérieur ne remplit pas ses obligations en matière de protection des Données à Caractère Personnel, Scaleway demeure pleinement responsable devant le Client de l'exécution par le Sous-traitant Ultérieur de ses obligations.

7.3 Scaleway s'assure que chaque Sous-traitant Ultérieur est soumis à des obligations de confidentialité adéquates et qu'il s'engage à respecter les obligations du présent Accord de Sous-traitance pour le compte et selon les instructions du Client, par un accord écrit ayant un contenu similaire à celui de l'Accord de Sous-traitance.

Article 8 - Mesures de sécurité

8.1 Scaleway s'engage à adopter des Mesures de Sécurité conformes aux dispositions de la Réglementation relative à la Protection des Données ;

8.2 Plus particulièrement, Scaleway, s'engage :

a) à adopter l'ensemble des mesures techniques et organisationnelles décrites dans sa Politique de Sécurité des Systèmes d'Information (PSSI), disponible sur son site web ;

b) à envoyer à la demande du Client des informations relatives notamment aux mesures physiques, organisationnelles et techniques adoptées dans le cadre des Services pour le Traitement des Données à Caractère Personnel par Scaleway et ses propres Sous-traitants Ultérieurs éventuels, ainsi dans la mesure du raisonnable, que toute autre information complémentaire éventuellement demandée par le Client en relation avec les mesures physiques, techniques et organisationnelles mises en œuvre en lien avec le Traitement des Données à Caractère Personnel.

Article 9 - Violation des Données à Caractère Personnel

9.1 En cas de Violation des Données à Caractère Personnel, d'incidents susceptibles de compromettre la sécurité des Données à Caractère Personnel (par exemple : perte, dommage ou destruction des Données à Caractère Personnel, quel que soit le support ou format (papier, électronique ou autre), accès non autorisé de tiers aux Données à Caractère Personnel ou toute autre Violation des Données à Caractère Personnel), y compris de Violations des Données à Caractère Personnel découlant de la conduite des éventuels Sous-traitants Ultérieurs et/ou des Préposés de Scaleway, Scaleway :

a) informera dans les meilleurs délais le Client après en avoir pris connaissance, au moyen d'une notification écrite au Client et lui fournir les informations utiles afin de lui permettre en tant que responsable de cette obligation de notification, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente ; et

b) en collaboration avec le Client, adoptera immédiatement et, quoi qu'il en soit, sans retard injustifié, toute mesure s'avérant nécessaire afin de minimiser les risques de toute nature pesant sur les Données à Caractère Personnel et atténuer les possibles effets néfastes et de participer dans la limite du périmètre des services à la détermination de la cause.

9.2 Scaleway s'engage à tenir un registre énumérant les Violations de Données à Caractère Personnel relatives aux Données à Caractère Personnel objets du présent Accord de Sous-traitance, les circonstances y associées, leurs conséquences, les mesures adoptées afin d'y remédier ainsi que tout manquement commis au regard du présent Accord de Sous-traitance.

Article 10 - Droits des Personnes Concernées

10.1 Scaleway s'engage à collaborer avec le Client dans une mesure raisonnable afin de garantir la satisfaction, dans les délais et selon les modalités fixées par la loi, des demandes d'exercice de droits des Personnes Concernées prévus par la Réglementation relative à la Protection des Données, et plus généralement, afin de garantir le plein respect de la Réglementation relative à la Protection des Données. À cet égard, Scaleway s'engage à informer le Client, de toutes demandes d'exercice de droits formulées par les Personnes Concernées en question.

10.2 Scaleway met à disposition du Client des mécanismes pour exercer ses droits RGPD via sa Console de Gestion, ainsi que par mail aux adresses de contact mentionnées en Préambule.

Article 11 - Communication et transfert des Données à Caractère Personnel

11.1 Scaleway s'engage, dans le cadre du Traitement objet du présent Accord de Sous-traitance,

a) à s'abstenir de diffuser ou de communiquer les Données à Caractère Personnel à des tiers, y compris d'éventuels Sous-traitants Ultérieurs, à moins que la Réglementation relative à la Protection des Données ou le Contrat ne le prévoie expressément ou que le Client l'y autorise par écrit ; et

b) à s'abstenir de transmettre, diffuser ou stocker des Données à Caractère Personnel dans un pays tiers à l'Union Européenne, sans accord préalable et

exprès du Client. Si Scaleway est tenu de procéder à un transfert de Données à Caractère Personnel vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'État membre auquel elle est soumise, elle doit en informer le Client avant le traitement et justifier du caractère impératif de cette obligation, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

c) en cas de transfert de données personnelles hors de l'Union Européenne ou vers un pays ne bénéficiant pas de décision d'adéquation à :

- signer les Clauses Contractuelles Types conformément à la Réglementation relative à la Protection des Données ;

- prendre toutes les mesures techniques et organisationnelles nécessaires à la garantie de la protection et de la confidentialité des informations transmises conformément à la Réglementation relative à la Protection des Données.

Article 12 - Contrôle

12.1 Scaleway s'engage à fournir au Client, sur demande de celui-ci, tout document raisonnablement nécessaire afin de s'assurer qu'elle se conforme aux obligations nées du présent Accord de Sous-traitance.

12.2 Scaleway reconnaît que le Client pourra, sous réserve d'en notifier par écrit au préalable Scaleway dans un délai de 15 jours, à ses frais et au maximum une fois par an, faire évaluer par un tiers de confiance, reconnu en tant qu'auditeur indépendant des Parties et désigné par Scaleway, les mesures organisationnelles, techniques et de sécurité adoptées par Scaleway dans le cadre du Traitement des Données à Caractère Personnel pour l'exécution des services uniquement, dans les conditions qui seront définies par Scaleway et le Client et dans la limite du maintien des Services et de la confidentialité et sécurité des autres clients de Scaleway.

Article 13 - Fin du Contrat

Au terme du Contrat pour quelque motif que ce soit, Scaleway veillera à cesser immédiatement tout Traitement des Données à Caractère Personnel et à supprimer les Données à Caractère Personnel ainsi que les éventuelles copies de celles-ci, sauf si la conservation des Données à Caractère Personnel est imposée par la législation applicable, auquel cas cette conservation devra s'inscrire uniquement dans les limites strictement prévues par cette dernière. Il incombe donc au Client, dans le périmètre des Services de

s'assurer de la conservation de ses Données à Caractère Personnel préalablement au terme du Contrat.

Article 14 - Stipulations diverses

14.1 Le présent Accord de Sous-traitance est régi par le droit français. Les juridictions du ressort de la Cour d'Appel de Paris ont compétence exclusive pour connaître de tout litige découlant du présent Accord de Sous-traitance ou s'y rattachant.

14.2 Une modification du présent Accord de Sous-traitance ne sera valable que si elle est établie par écrit et signée par les représentants habilités du Responsable du Traitement et du Sous-traitant.

14.3 Le présent Accord de Sous-traitance ne peut être cédé à des tiers sans l'accord écrit préalable du Responsable du Traitement.

14.4 En cas de contradiction entre le présent Accord de Sous-traitance et les autres dispositions du Contrat, le présent Accord de Sous-traitance prévaudra en ce qui concerne les questions touchant au Traitement des Données à Caractère Personnel.

Contact :

- DPO de Scaleway : dpo@iliad.fr
- Équipe Privacy de Scaleway : privacy@scaleway.com
- Notification de violation de données : security@scaleway.com
- Politique de confidentialité de Scaleway : https://www.scaleway.com/fr/politique-confidentialite/

Annexe 4 : Data Processing Addendum (DPA) de OpenAI

Updated: February 15, 2024

Data processing addendum

This Data Processing Addendum ("**DPA**") governs OpenAI's processing of Customer Data (i) provided by Customer to OpenAI through OpenAI's API or any OpenAI services for businesses ("**API Services**") or (ii) pursuant to OpenAI's provision of the ChatGPT Enterprise service for businesses (the "**ChatGPT Enterprise Services**") (for purposes of this DPA, the API Services and ChatGPT Enterprise Services are together the "**Services**") under the terms of the OpenAI Business Terms (located at openai.com/policies/business-terms), Enterprise Agreement, or other agreement between Customer and OpenAI governing Customer's use of the Services (the "**Agreement**") and is hereby incorporated into the Agreement. If and to the extent language in this DPA conflicts with the Agreement, the conflicting terms in this DPA shall control. Capitalized terms not defined in this DPA have the meaning set forth in the Agreement. For the purposes of this DPA only, "**Customer**" includes any affiliate entity of Customer's that (a) has entered into an Order Form with OpenAI and that (b) directly or indirectly, through one or more intermediaries controls, is controlled by, or is under common control with Customer.

If Customer is located in the EEA or Switzerland, OpenAI Ireland Ltd will provide the Services and contract with Customer. If Customer is located in the UK or anywhere else other than the EEA or Switzerland, OpenAI, LLC will provide the Services and contract with Customer. For the purposes of this DPA, "**OpenAI**" refers to the OpenAI entity contracting with Customer.

OpenAI and Customer each agree to comply with their respective obligations under applicable data privacy and data protection laws (collectively, "**Data Protection Laws**") in connection with the Services. Data Protection Laws may include, depending on the circumstances, Cal. Civ. Code §§ 1798.100 et seq., as amended by the California Privacy Rights Act of 2020 (the California Consumer Privacy Act) ("**CCPA**"), Colo. Rev. Stat. §§ 6-1-1301 et seq. (the Colorado Privacy Act) ("**CPA**"), Connecticut's Data Privacy Act ("**CTDPA**"), Utah Code Ann. §§ 13-61-101 et seq. (the Utah Consumer Privacy Act) ("**UCPA**"), VA Code Ann. §§ 59.1-575 et seq. (the Virginia Consumer Data Protection Act) ("**VCDPA**") (collectively "**U.S. Privacy Laws**"), and the United Kingdom and/or European Union General Data Protection Regulation (Regulation (EU) 2016/679) (collectively the "**GDPR**"), and applicable subordinate legislation and regulations implementing those laws.

In connection with the Agreement, Customer is the person that determines the purposes and means for which Customer Data (as defined below) is processed (a "**Data Controller**"), whereas OpenAI processes Customer Data in accordance with the Data Controller's instructions and on behalf of the Data Controller (as a "**Data Processor**"). "**Data Controller**" and "**Data Processor**" also mean the equivalent concepts under Data Protection Laws. For the purposes of the Agreement and this DPA, (i) "**Personal Data**" has the meaning assigned to the term "personal data" or "personal information" under applicable Data Protection Laws; and (ii) "**Customer Data**" means Personal Data that Customer provides to OpenAI that OpenAI processes on behalf of Customer to provide the Services. OpenAI will process Customer Data as Customer's Data Processor to provide or maintain the Services and for the purposes set forth in this DPA, the Agreement and/or in any other applicable agreements between Customer and OpenAI.

1. Processing Requirements

As a Data Processor, OpenAI agrees to:

a. process Customer Data only (i) on Customer's behalf for the purpose of providing and supporting OpenAI's Services (including to provide insights, reporting, analytics, and platform abuse,

trust and safety monitoring); (ii) in compliance with the written instructions received from Customer; and (iii) in a manner that provides no less than the level of privacy protection required of it by Data Protection Laws;

b. promptly inform Customer in writing if OpenAI cannot comply with the requirements of this DPA;

c. not provide Customer with remuneration in exchange for Customer Data from Customer. The parties acknowledge and agree that Customer has not "sold" (as such term is defined by the CCPA) Customer Data to OpenAI;

d. not "sell" (as such term is defined by U.S. Privacy Laws) or "share" (as such term is defined by the CCPA) Personal Data;

e. inform Customer promptly if, in OpenAI's opinion, an instruction from Customer violates applicable Data Protection Laws;

f. require (i) persons employed by it and (ii) other persons engaged to perform on OpenAI's behalf to be subject to a duty of confidentiality with respect to the Customer Data and to comply with the data protection obligations applicable to OpenAI under the Agreement and this DPA;

g. engage the organizations or persons listed at https://platform.openai.com/subprocessors(opens in a new window) to process Customer Data (each "**Subprocessor,**" and the list at the foregoing URL, the "**Subprocessor List**") to help OpenAI satisfy its obligations in accordance with this DPA or to delegate all or part of the processing activities to such Subprocessors. Customer hereby consents to the use of such Subprocessors. If Customer subscribes to email notifications as provided on the Subprocessor List website, then OpenAI will notify Customer of any changes OpenAI intends to make to the Subprocessor List at least 15 days before the changes take effect (which may be via email, a posting, or notification on an online portal for our services or other reasonable means). In the event that Customer does not wish to consent to the use of such additional Subprocessor, Customer may notify OpenAI that Customer does not consent within fifteen (15) days on reasonable grounds relating to the protection of Customer Data by following the instructions set forth in the Subprocessor List or by contacting privacy@openai.com. In such case, OpenAI shall have the right to cure the objection through one of the following options: (i) OpenAI will cancel its plans to use the Subprocessor with regards to processing Customer Data or will offer an alternative to provide its Services or services without such Subprocessor; (ii) OpenAI will take the corrective steps requested by Customer in Customer objection notice and proceed to use the Subprocessor; (iii) OpenAI may cease to provide, or Customer may agree not to use whether temporarily or permanently, the particular aspect or feature of the OpenAI Services or services that would involve the use of such Subprocessor; or (iv) Customer may cease providing Customer Data to OpenAI for processing involving such Subprocessor. If none of the above options are commercially feasible, in OpenAI's reasonable judgment, and the objection(s) have not been resolved to the satisfaction of the parties within thirty (30) days of OpenAI's receipt of Customer's objection notice, then either party may terminate any subscriptions, order forms or usage regarding the Services that cannot be provided without the use of the new Subprocessor for cause and in such case, Customer will be refunded any pre-paid fees for the applicable subscriptions, order forms or usage to the extent they cover periods or terms following the date of such termination. Such termination right is Customer's sole and exclusive remedy if Customer objects to any new Subprocessor. OpenAI shall enter into contractual arrangements with each Subprocessor binding them to provide a comparable level of data protection and information security to that provided for herein. Subject to the limitations of liability included in the Agreement, OpenAI agrees to be liable for the acts and omissions of its Subprocessors to the same extent OpenAI would be liable under the terms of the DPA if it performed such acts or omissions itself;

h. upon reasonable request no more than once per year, provide Customer with OpenAI's privacy and security policies and other such information necessary to demonstrate compliance with the obligations set forth in this DPA and applicable Data Protection Laws;

i. where required by law and upon reasonable notice and appropriate confidentiality agreements, cooperate with assessments, audits, or other steps performed by or on behalf of

Customer at Customer's sole expense and in a manner that is minimally disruptive to OpenAI's business that are necessary to confirm that OpenAI is processing Customer Data in a manner consistent with this DPA. Where permitted by law, OpenAI may instead make available to Customer a summary of the results of a third-party audit or certification reports relevant to OpenAI's compliance with this DPA. Such results, and/or the results of any such assessments, audits, or other steps shall be the Confidential Information of OpenAI;

j. to the extent that Customer permits or instructs OpenAI to process Customer Data subject to U.S. Privacy Laws in a de-identified, anonymized, and/or aggregated form as part of the Services, OpenAI shall (i) adopt reasonable measures to prevent such deidentified data from being used to infer information about, or otherwise being linked to, a particular natural person or household; (ii) not attempt to re-identify the information, except that OpenAI may attempt to reidentify the information solely for the purpose of determining whether its de-identification processes comply with Data Protection Laws or are functioning as intended; and (iii) before sharing de-identified data with any other party, including Subprocessors, contractually obligate any such recipients to comply with the requirements of this provision;

k. where the Customer Data is subject to the CCPA, not (i) retain, use, disclose, or otherwise process Customer Data except as necessary for the business purposes specified in the Agreement or this DPA; (ii) retain, use, disclose, or otherwise process Customer Data in any manner outside of the direct business relationship between OpenAI and Customer; or (iii) combine any Customer Data with Personal Data that OpenAI receives from or on behalf of any other third party or collects from OpenAI's own interactions with individuals, provided that OpenAI may so combine Customer Data for a purpose permitted under the CCPA if directed to do so by Customer or as otherwise permitted by the CCPA;

l. where required by law, grant Customer the rights to (i) take reasonable and appropriate steps to ensure that OpenAI uses Customer Data in a manner consistent with Data Protection Laws by exercising the audit provisions set forth in this DPA above; and (ii) stop and remediate unauthorized use of Customer Data, for example by requesting that OpenAI provide written confirmation that applicable Customer Data has been deleted.

2. Notice to Customer

OpenAI will inform Customer if OpenAI becomes aware of:

a. any legally binding request for disclosure of Customer Data by a law enforcement authority, unless OpenAI is otherwise forbidden by law to inform Customer, for example to preserve the confidentiality of an investigation by law enforcement authorities;

b. any notice, inquiry or investigation by an independent public authority established by a member state pursuant to Article 51 of the GDPR (a "Supervisory Authority") with respect to Customer Data; or

c. any complaint or request (in particular, requests for access to, rectification or blocking of Customer Data) received directly from Customer's data subjects. OpenAI will not respond to any such request without Customer's prior written authorization.

3. Assistance to Customer

OpenAI will provide reasonable assistance to Customer regarding:

a. information necessary, taking into account the nature of the processing, to respond to requests received pursuant to Data Protection Laws from Customer's data subjects in respect of access to or the rectification, erasure, restriction, portability, objection, blocking or deletion of Customer Data that OpenAI processes for Customer. In the event that a data subject sends such a request directly to OpenAI, OpenAI will promptly send such request to Customer;

b. the investigation of any breach of OpenAI's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Customer Data processed by OpenAI for Customer (a "Personal Data Breach"); and

c. where appropriate, the preparation of data protection impact assessments with respect to the processing of Customer Data by OpenAI and, where necessary, carrying out consultations with any supervisory authority with jurisdiction over such processing.

4. Required Processing

If OpenAI is required by Data Protection Laws to process any Customer Data for a reason other than in connection with the Agreement, OpenAI will inform Customer of this requirement in advance of any such processing, unless legally prohibited.

5. Security

OpenAI will:

a. maintain reasonable and appropriate organizational and technical security measures, including but not limited to those measures described in Exhibit B to this DPA (including with respect to personnel, facilities, hardware and software, storage and networks, access controls, monitoring and logging, vulnerability and breach detection, incident response, and encryption) to protect against unauthorized or accidental access, loss, alteration, disclosure or destruction of Customer Data and to protect the rights of the subjects of that Customer Data;

b. take appropriate steps to confirm that OpenAI personnel are protecting the security, privacy and confidentiality of Customer Data consistent with the requirements of this DPA; and

c. notify Customer of any Personal Data Breach by OpenAI, its Subprocessors, or any other third parties acting on OpenAI's behalf without undue delay after OpenAI becomes aware of such Personal Data Breach.

6. Obligations of Customer

a. Customer represents, warrants and covenants that it has and shall maintain throughout the term all necessary rights, consents and authorizations to provide the Customer Data to OpenAI and to authorize OpenAI to use, disclose, retain and otherwise process Customer Data as contemplated by this DPA, the Agreement and/or other processing instructions provided to OpenAI.

b. Customer shall comply with all applicable Data Protection Laws.

c. Customer shall reasonably cooperate with OpenAI to assist OpenAI in performing any of its obligations with regard to any requests from Customer's data subjects.

d. Without prejudice to OpenAI's security obligations in Section 5 of this DPA, Customer acknowledges and agrees that it, rather than OpenAI, is responsible for certain configurations and design decisions for the services and that Customer, and not OpenAI, is responsible for implementing those configurations and design decisions in a secure manner that complies with applicable Data Protection Laws.

e. Customer shall not provide Customer Data to OpenAI except through agreed mechanisms. For example, Customer shall not include Customer Data other than technical contact information, or in technical support tickets, transmit user Customer Data to OpenAI by email. Without limitation to the foregoing, Customer represents, warrants and covenants that it shall only transfer Customer Data to OpenAI using secure, reasonable and appropriate mechanisms, to the extent such mechanisms are within Customer's control.

f. Customer shall not take any action that would (i) render the provision of Customer Data to OpenAI a "sale" under U.S. Privacy Laws or a "share" under the CCPA (or equivalent concepts under U.S. Privacy Laws); or (ii) render OpenAI not a "service provider" under the CCPA or "processor" under U.S. Privacy Laws.

7. International Data Transfers

a. OpenAI Ireland Ltd. will process Customer Data provided by Customer that originates in the EEA or Switzerland. To the extent that OpenAI Ireland Ltd transfers Customer Data to other OpenAI affiliates in jurisdictions that do not provide the same level of data protection, it will do so on the basis of intra-group agreements that incorporate appropriate transfer mechanism provisions to

protect Customer Data. Such mechanisms may include the Standard Contractual Clauses adopted by the EU Commission on June 4, 2021 (as may be amended, updated or replaced from time to time) ("**EU SCCs**") or an adequacy decision issued by the European Commission under Article 45 GDPR.

b. OpenAI OpCo, LLC will process Customer Data provided by Customer located in the UK in accordance with the EU SCCs as amended by the UK addendum to the EU SCCs issued by the Information Commissioner under section 119A(1) of the Data Protection Act 2018 ("**UK Addendum**") which are deemed entered into (and incorporated into this DPA by this reference) and completed as follows (each as amended by the UK Addendum, where relevant and applicable):i. Module Two (Controller to Processor) of the EU SCCs apply when Customer is a controller and OpenAI is processing Customer Data as a processor.ii. Module Three (Processor to Sub-Processor) of the EU SCCs apply when Customer is a processor and OpenAI is processing Customer Data as a sub-processor.

c. For each module of the EU SCCs, where applicable, the following applies: i. The optional docking clause in Clause 7 does not apply;ii. In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Section 1(g) of this DPA.iii. In Clause 11, the optional language does not apply;iv. All square brackets in Clause 13 are hereby removed;v. In Clause 17 (Option 1), the EU SCCs will be governed by the laws of England and Wales;vi. In Clause 18(b), disputes will be resolved before the courts of England and Wales;vii. Exhibit A to this DPA contains the information required in Annex I and Annex III of the EU SCCs;viii. Exhibit B to this DPA contains the information required in Annex II of the EU SCCs; and

d. The parties will comply with the terms of Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B1.0 . The parties also agree (i) that the information included in Part 1 of the UK Addendum is as set out in Exhibit A to this DPA and (ii) that either party may end the UK Addendum as set out in Section 19 of the UK Addendum.

8. Term; Data Return and Deletion

This DPA shall remain in effect as long as OpenAI carries out Customer Data processing operations on Customer's behalf or until the termination of the Agreement (and all Customer Data has been returned or deleted in accordance with this DPA). OpenAI will retain API Service Customer Data sent through the API for a maximum of thirty (30) days, after which it will be deleted, except where OpenAI is required to retain copies under applicable laws, in which case OpenAI will isolate and protect that Customer Data from any further processing except to the extent required by applicable laws. OpenAI will retain ChatGPT Enterprise Service Customer Data during the term of the Agreement, unless otherwise stated in the Agreement or Order Form. On the termination of the DPA, OpenAI will direct each Subprocessor to delete the Customer Data within thirty (30) days of the DPA's termination, unless prohibited by law. For clarity, OpenAI may continue to process information derived from Customer Data that has been deidentified, anonymized, and/or aggregated such that the data is no longer considered Personal Data under applicable Data Protection Laws and in a manner that does not identify individuals or Customer to improve OpenAI's systems and services.

Exhibit A

A. LIST OF PARTIES

A. LIST OF PARTIES

Data exporter(s): the Services customer identified on the applicable Services registration documents

Data importer(s):

Name: OpenAI OpCo, LLC

Address: 3180 18th St., San Francisco, CA 94110

Contact Person's name, position and contact details:

Head of Commercial Legalprivacy@openai.comActivities relevant to the data transferred under these Clauses: The performance of the services described in the agreement to which this is attached.

Signature and date:

Role (controller/processor):

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Users of data exporters applications.

Categories of personal data transferred

Name, contact information, demographic information, or other information provided by the user in unstructured data.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No sensitive data is intended to be transferred unless the user includes it unexpectedly in unstructured data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous.

Nature of the processing

The performance of the services described in the agreement to which this exhibit is attached.

Purpose(s) of the data transfer and further processing

The performance of the services described in the agreement to which this exhibit is attached.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

During the term of the agreement

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The performance of the services described in the agreement to which this exhibit is attached.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Information Commissioner's Office ("ICO").

Exhibit B

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

INTRODUCTION

OpenAI's mission is to deploy safe and responsible AI at scale for the benefit of all. In accordance with this mission, OpenAI maintains an information security program designed to safeguard its systems, data, and Customer Data. This Exhibit describes the information security program and security standards that OpenAI maintains with respect to the Services and handling of data submitted by or on behalf of Customer of the Services (the "Customer Data"). Capitalized terms not defined in this Exhibit have the meanings given in the DPA or Agreement.

ChatGPT Enterprise is a new OpenAI Service and so certain technical or security measures below apply differently to ChatGPT Enterprise; in each case that difference is noted in *italicized* language. "ChatGPT Enterprise" is the version of OpenAI's AI-powered ChatGPT language model that is available to enterprises.

To learn more about OpenAI's technical and organizational security measures to protect Customer Data, see the OpenAI Trust Portal at https://trust.openai.com/(opens in a new window) **(the "Trust Portal"). The Security Measures below include the subset of the information available in the Trust Portal which applies to this DPA.**

SECURITY MEASURES

Corporate Identity, Authentication, and Authorization Controls. OpenAI maintains industry best practices for authenticating and authorizing internal employee and service access, including the following measures:

- OpenAI uses single sign-on (SSO) to authenticate to third-party services used in the delivery of the Services. Role Based Access Controls (RBAC) are used when provisioning internal access to the Services;
- Mandatory multi-factor authentication is used for authenticating to OpenAI's identity provider.
- Unique login identifiers are assigned to each user;
- Established review and approval processes for any access requests to services storing Customer Data;
- Periodic access audits designed to ensure access levels are appropriate for the roles each user performs;
- Established procedures for promptly revoking access rights upon employee separation;
- Established procedures for reporting and revoking compromised credentials such as passwords and API keys); and
- Established password reset procedures, including procedures designed to verify the identity of a user prior to a new, replacement, or temporary password.

Customer Identity, Authentication, and Authorization Controls. OpenAI maintains industry best practices for authenticating and authorizing customers to the Services, including the following measures:

- Use of a third-party identity access management service to manage Customer identity, meaning OpenAI does not store user-provided passwords on users' behalf; and
- Logically separating Customer Data by organization account using unique identifiers. Within an organization account, unique user accounts are supported.
- Cloud Infrastructure and Network Security. OpenAI maintains industry best practices for securing and operating its cloud infrastructure, including the following measures:
- Separate production and non-production environments;
- Primary backend resources are deployed behind a VPN.
- The Services are routinely audited for security vulnerabilities.
- Application secrets and service accounts are managed by a secrets management service;
- Network security policies and firewalls are configured for least-privilege access against a pre-established set of permissible traffic flows. Non-permitted traffic flows are blocked; and
- Services logs are monitored for security and availability.

System and Workstation Control. OpenAI maintains industry best practices for securing OpenAI's corporate systems, including laptops and on-premises infrastructure, including:

- Endpoint management of corporate workstations;
- Endpoint management of mobile devices;
- Automatic application of security configurations to workstations;
- Mandatory patch management; and
- Maintaining appropriate security logs.

Data Access Control. OpenAI maintains industry best practices for preventing authorized users from accessing data beyond their authorized access rights and for preventing the unauthorized input, reading, copying, removal, modification, or disclosure of data. Such measures include the following:

- Employee access to the Services follows the principle of least privilege. Only employees whose job function involves supporting the delivery of Services are credentialed to the Services environment; and
- Customer Data submitted to the Services is only used in accordance with the terms of the DPA, Agreement, and any other applicable contractual agreements in place with Customer.

Disclosure Control. OpenAI maintains industry best practices for preventing the unauthorized access, alteration, or removal of data during transfer, and for securing and logging all transfers. Such measures include:

- Encryption of data at rest in production datastores using strong encryption algorithms;
- Encryption of data in transit;
- Audit trail for all data access requests for production datastores;
- Full-disk encryption required on all corporate workstations;
- Device management controls required on all corporate workstations;
- Restrictions on use of portable or removable media; and
- Customer Data can be deleted upon request.

Availability control. OpenAI maintains industry best practices for maintaining Services functionality through accidental or malicious intent, including:

- Ensuring that systems may be restored in the event of an interruption;
- Ensuring that systems are functioning and faults are reported; and
- Anti-malware and intrusion detection/prevention solutions implemented comprehensively across our environment.

Segregation control. OpenAI maintains industry best practices for separate processing of data collected for different purposes, including:

- Logical segregation of Customer Data;
- Restriction of access to data stored for different purposes according to staff roles and responsibilities;
- Segregation of business information system functions; and
- Segregation of testing and production information system environments.

Risk Management. OpenAI maintains industry best practices for detecting and managing cybersecurity risks, including:

- Threat modeling to document and triage sources of security risk for prioritization and remediation;
- Penetration testing is conducted on the Services at least annually, and any remediation items identified are resolved as soon as possible on a timetable commensurate with the associated risk. Upon request, OpenAI will provide summary details of the tests performed and whether the identified issues have been resolved;;
- Annual engagements of a qualified, independent external auditor to conduct periodic reviews of OpenAI's security practices against recognized audit standards, including SOC 2 Type II certification audits. Upon reasonable request, OpenAI will provide summary details; and
- A vulnerability management program designed to ensure the prompt remediation of vulnerabilities affecting the Services.

Personnel. OpenAI maintains industry best practices for vetting, training, and managing personnel with respect to security matters, including:

- Background checks, where legally permissible, of employees with access to Customer Data or supporting other aspects of the Services;
- Annual security training for employees, and supplemental security training as appropriate.

Physical Access Control. OpenAI maintains industry best practices for preventing unauthorized physical access to OpenAI facilities, including:

- Physical barrier controls including locked doors and gates;
- 24-hour on-site security guard staffing;
- 24-hour video surveillance and alarm systems, including video surveillance of common areas and facility entrance and exit points;
- Access control systems requiring biometrics or photo-ID badge and PIN for entry to all OpenAI facilities by OpenAI personnel;
- Visitor identification,sign-in and escort protocols; and
- Logging of facility exits and entries.

Third Party Risk Management. OpenAI maintains industry best practices for managing third party security risks, including with respect to any subprocessor or subcontractor to whom OpenAI provides Customer Data, including the following measures:

- Written contracts designed to ensure that any agent agrees to maintain reasonable and appropriate safeguards to protect Customer Data; and
- Vendor Security Assessments: All third parties undergo a formal vendor assessment process maintained by OpenAI's Security team.

Security Incident Response. OpenAI maintains a security incident response plan for responding to and resolving events that compromise the confidentiality, availability, or integrity of the Services or Customer Data including the following:

- OpenAI aggregates system logs for security and general observability from a range of systems to facilitate detection and response; and
- If OpenAI becomes aware that a Personal Data Breach has occurred, OpenAI will notify Customer in accordance with the DPA.

Security Evaluations. OpenAI performs regular security and vulnerability testing to assess whether key controls are implemented properly and are effective as measured against industry security standards and its policies and procedures and to ensure continued compliance with obligations imposed by law, regulation, or contract with respect to the security of Customer Data as well as the maintenance and structure of OpenAI's information systems_._

Annexe 5 : Privacy Policy de Contabo

1. General information

If you would like an introduction to the topic of data protection and the General Data Protection Regulation, you may find further information e.g. on the website of the Federal Data Protection Officer, available at https://www.bfdi.bund.de/DE/Home/home_node.html (German language only).

This privacy policy will provide you information on how we use your personal data.

2. Information regarding controller and data protection officer

2.1. Contabo GmbH, Aschauer Straße 32a, 81549 München is the 'controller' and as such responsible for the processing of your personal data. You can reach us for general questions either by phone at +49 /(89) /3564717-71 or by e-mail https://contabo.com
.

2.2. For questions on data protection or exercising your rights under data protection law (see Section /4), you may contact our data protection officer either by post at Herrn Rechtsanwalt Dr. Karsten Kinast, LL.M. KINAST
Rechtsanwaltsgesellschaft mbH, Hohenzollernring 54, 50672 Köln or by email at datenschutzbeauftragter@contabo.de

3. Activities, in which we process your personal data

3.1. Visiting our website

If you visit our website without logging in, registering or otherwise filling in the input fields on the website, we process your personal data as follows:

3.1.1. For the purpose of providing our website, we process the IP address, access time, browser information, operating system, language setting, screen resolution, the page or file accessed, as well as the access status (successful or error code) for each page view of all website visitors. š
The processing is technically necessary to enable the use of our website (Art. 6 (1) lit. b GDPR). š
The data is deleted after the end of your visit to our website, unless specific data is further processed for one or more of the purposes described in this privacy notice.

3.1.2. For the purpose of detecting and blocking attacks on our website and the technical infrastructure (e.g. hacking, denial of service attack), we process personal data including identification data, connection data or localization data (including IP addresses). š
This processing is necessary to pursue our legitimate interest to take protective measures against attacks (Article 6 (1) lit. f GDPR).

The personal data will be processed by Cloudflare Inc., 101 Townsend St San Francisco, CA 94107 under a data processing agreement (Art. 28 GDPR).

3.1.3. The data is deleted no later than two (2) years after the end of your visit to our website, unless an attempted attack is detected. In the event of a detected attempted attack from your point of access, the data will be further processed for technical and, if necessary, legal processing.š
Visitors of our website have the right to object to the use of these cookies as described below in sect. /4.2.3.

3.1.4. For the purpose of providing our website we use the cloud platform Vercel, provided by Vercel Inc., 340 S Lemon Ave #4133 Walnut, CA 91789 under a data processing agreement (Art. 28 GDPR).
Each visit to our website will be handled or delivered through Vercel who processes information, which may include; IP addresses, system configuration information, and other information

about traffic to and from our website, for the purpose of operating, maintaining and improving service. This data can help to detect new threats, identify malicious third parties, and provide more robust security protection.
The processing of this data is technically necessary to enable the use of our website (Art. 6 (1) lit. b GDPR).

3.1.5. We use cookies on our website. Cookies are small text files. They allow us to store specific visitor-related information in the context of the use of our website. You can find details of our cookie policy at: https://contabo.com/en/legal/cookie-policy/

3.2. Website Registration

a) For the purposes of providing you access to and use of the functionality of our website that requires registration, such as the user and customer portal or leaving comments on the website, we process the IP address, first name, last name, gender, postal address and country, email address, status as private individual or business representative, and in case of business registration also the trade-name of the business and tax ID number or similar business identification information.

This processing is necessary to enable the use of some functionality of our website (Art. 6 (1) lit. b GDPR). For individuals who are not party to the contract, but represent a company, the legal basis is Art. 6 (1) lit. f GDPR.

We will retain the data until you ask us to delete your user account. After that the processing of the data will be restricted and no longer used for identification and access to the functions of the website requiring registration.

Individuals representing a business have the right to object to data processing as described below in sect. /4.2.3.

b) For the purpose of verifying customer identity, we process the IP address, first name, last name, gender, postal address and country, email address, status as private individual or business representative, and in case of business registration also the trade-name of the business and tax ID number or similar business identification information.

This processing is necessary to ensure the identity of our customer and to enable the use of our website (Art. 6 (1) lit. b GDPR). For individuals who are not party to the contract, but represent a company, the legal basis is Art. 6 (1) lit. f GDPR.

We will retain the data until you ask us to delete your user account. After that the processing of the data will be restricted and no longer used for identification and access to the functions of the website requiring registration.

Individuals representing a business have the right to object to data processing as described below in sect. 4.2.3.

3.3. Website comment function

For the purpose of displaying the username together with a comment left on our website or the blog, as well as identifying the author of a comment in case of later complaints about the content of the comment, we process the IP-address of the machine used to send the comment, and if available the email-address and/or username of the author of the comment.

Registered users may subscribe to comment feeds, in which case we use the email-address to send new comments and responses by email.

The processing is necessary to pursue our legitimate interest to protect ourselves and our users from unlawful content on our website and enable a community environment by displaying the usernames (Art. 6 (1) lit. f GDPR).

We retain the IP-addresses, the email-address and/or username for as long as the comment is stored and visible on our website, or until the registered user has unsubscribed from the comment feed.

Authors of comments have the right to object to data processing as described below in sect. /4.2.3. This right may also be exercised by using the anonymous commenting function.

3.4. Email advertisement

For the purpose of processing email communication with customers about industry news and advertisement for our own products and services, such as information about promotions, new product launches and new offers, we process the email-address of our customers.

This processing is based on the customer's consent (Art. 6 (1) lit. a GDPR).

We retain the email-address until consent is withdrawn. The processing of the email-address for this purpose is restricted after withdrawal of consent, and the email-address is deleted unless it is also processed for other purposes.

The customer has the right to withdraw consent as described below in sect. 4.2.4. Subscriber may also withdraw consent by unsubscribing from the mailing by using the "unsubscribe" link contained in every advertisement mailing.

3.5. Email newsletters

For the purpose of sending email newsletters with information about industry news and advertisement for our own products and services, such as information about promotions, new product launches and new offers, we process the email-address of the subscriber.

This processing is based on the subscriber's consent (Art. 6 (1) lit. a GDPR).

We retain the email-address until consent is withdrawn. The processing of the email-address for this purpose is restricted after withdrawal of consent, and the email-address is deleted unless it is also processed for other purposes.

The subscriber has the right to withdraw consent as described below in sect. /4.2.4. Subscriber may also withdraw consent by unsubscribing from the newsletters by using the "unsubscribe" link contained in every newsletter mailing.

3.6 Application for job vacancy

By submitting an application on our recruiting page or to us via email, the applicant declares that he wishes to take up an employment with us. We process and store all personal data provided by the applicant exclusively for the purpose of the job search/application.

In particular the following data are collected: name (first and last name), e-mail address, telephone number, LinkedIn-Profile (optional), channel (how the applicant became aware of us).

You also have the option to upload documents such as cover letter, CV and references. These may include further personal data such as date of birth, address, etc.

If provided by the applicant, we also process special categories of personal data, for example information on handicaps, ethnic origin or biometric data (handwritten signature).

The processing of the aforementioned personal data is necessary as a pre-contractual measure. We use the provided personal data for the application process (assessment and qualification for the position). The processing is based on Art. 6 (1) lit. b, Art. 88 GDPR in connection

with sect. 26 BDSG.

Where special categories of data are provided voluntarily by the applicant, processing is based on Art. 9 (2) lit. a GDPR. By providing the special categories of personal data concerned, the applicant consents to the processing.

Data transmitted as part of your application will be transferred using TLS encryption and stored in a database. This database is operated by Personio GmbH (Rundfunkplatz 4, 80335 München), which offers a human resource and applicant management software solution (https://www.personio.com/legal-notice/). In this context, Personio is our processor under article 28 of the GDPR. In this case, the processing is based on an agreement for the processing of orders between us as the controller and Personio.

The data contained in the application letter is made available to our HR-department and the decision makers for the respective job vacancy.

The personal data is stored, as a rule, exclusively for the purpose of filling the vacancy for which you have applied.

We retain the data until six months after a decision on filling the job vacancy is communicated to the applicant. After this period we will delete or anonymize your data. In case of anonymization, the data will only be available to us in the form of so-called metadata, without any direct personal reference, for statistical analysis (for example, share of male and/or female applicants, number of applications per specified period of time etc.).

The applicant has the right to withdraw consent to processing of voluntarily provided special categories of data as described below in sect. /4.2.4.

Should you be offered and accept a position with us during the application process, we will store the personal data collected as part of

the application process for at least the duration of your employment.

3.7 Talent pool

For possible consideration for future job vacancies, we process all personal data provided by applicants either for a job application (see above sect. /3.6) or as an unsolicited application (concerning the categories of data described above in sect. /3.6) to decide on whether to consider an applicant for any available job vacancies.

The processing is based on the applicant´s express consent (Art. 6 (1) lit. a, Art. 9 (2) lit. a GDPR).

We retain the data for 6 month or until consent is withdrawn, whichever is earlier. The application letter and the data contained therein is then erased, returned to the applicant or destroyed, unless the applicant has renewed consent (e.g. upon our request) or data is further processed for employment purposes.

The applicant has the right to withdraw consent to processing as described below in sect. /4.2.4

3.8. Order processing

For the purpose of processing customer orders of our products and services and commissioning the products and services for delivery, we process the personal data provided during website registration (see above sect. /3.2) and the status of the customer's payments.

The processing is necessary to perform the contract with the customer (Art. 6 (1) lit. b GDPR).

We retain the personal data until after termination of all contracts with the customer. Then processing for this purpose is restricted. The data is deleted after all mandatory retention periods have expired.

3.9. Fraud prevention

For the purpose of protecting against attempts at payment fraud or misuse of our products and services for unlawful uses (e.g. spamming, hosting illegal content), we process the personal data provided during website registration (see above sect. 3.2). We transfer IP address to Maxmind Inc., seated in 14 Spring Street, 3rd Floor, Waltham, MA 02451 USA for the purpose of determining if this is a proxy address.

The processing is necessary to pursue our legitimate interest of fraud prevention (Art. 6 (1) lit. f GDPR).

We will retain the data until you ask us to delete your user account. After that the processing of the data will be restricted and no longer used for fraud prevention.

3.10. Payment processing

For the purpose of processing payments for products and services we process the personal data provided for website registration (see above sect. /3.2) and the account information provided by the customer, the products and services ordered and the amounts incurred. Unless the customer prepays the remuneration for the entire contract duration by bank transfer, the data is transferred to the respective payment processing provider selected by the customer, for example PayPal (Europe) S.à.r.l & Cie, S.C.A., 22-24 Boulevard Royal, L-2449 Luxembourg and Stripe Payments Europe Ltd., 1 Grand Canal Street Lower, Dublin 2, Ireland.

The processing and transfer are necessary to perform the contract with the customer (Art. 6 (1) lit. b GDPR).

We retain the account information for the lifetime of the customer account + 6 months. Then processing is restricted for this purpose and deleted after all mandatory retention periods have expired.

3.11. Customer and product support

To process all customer or product support inquiries that reach us by email or phone, we process the name, first name, email address, telephone number and other personal data communicated in the e-mail as well as information on the content of the request.

The processing is necessary to handle the request or inquiry (Article 6 (1) lit. b GDPR).

Depending on the content of the request, processing will be restricted to processing for the specific purpose of the request immediately after completing the processing of the request. The data is deleted after all mandatory retention periods have expired.

4. Your data subject rights

4.1. You may at any time exercise your rights as a data subject by contacting us by mail or e-mail to our address mentioned in section 2.2. Please keep in mind that we do not answer any inquiries about personal data by telephone, because generally the identity of the caller cannot be determined with sufficient certainty.

4.2. You have the following rights with respect to your personal data:

4.2.1. You may exercise your right of access (Art. 15 GDPR), the right to rectification (Art. 16 GDPR), the right to erasure (Art. 17 GDPR) and the right to restriction of processing, i. /e. blocking for certain purposes, (Art. 18 GDPR) at any time, if the respective statutory prerequisites are met.

4.2.2. Your right to data portability (Art. 20 GDPR) also stipulates that, if the statutory prerequisites are met, you may demand that your personal data stored by us will be transferred to you – or insofar as technically feasible, to another controller designated by you –

in a structured, commonly used and machine-readable format.

4.2.3. You have the right to object to processing (Art. 21 GDPR) for some processing purposes, in particular advertising purposes. Insofar as we process your data based on a balancing of interests (pursuant to Art. 6 (1) lit. f GDPR), you have the right to object to this processing at any time based on grounds related to your particular situation. Such grounds may be compelling in particular, if they give special weight to your interests, which thereby outweigh our interests, for example if these reasons are not known to us and therefore could not be taken into account in the balancing of interests. You may object to processing by sending us an email to the address stated in sect. /2.2, and we may advise you of additional ways to object to processing for each specific processing activity in sect. /3.

4.2.4. You have the right to withdraw consent you have given us to process your personal data (Art. 7 (3) GDPR). You may withdraw your consent at any time and without need to give any reason, either for all processing or limited to specific processing of your data that is based on your consent. Withdrawal of consent will be effective immediately and for any future processing. The lawfulness of processing before withdrawal of consent remains unaffected. You may withdraw consent by sending us an email to the address stated in sect. /2.2, and we may advise you of additional ways to withdraw consent for each specific processing activity in sect. /3.

4.3. You also have the right to contact the competent data protection supervisory authority for questions or complaints regarding the processing of your personal data. You may find information on how to contact the Bavarian supervisory authority at https://www.lda.bayern.de/de/kontakt.html
(German language only).

Annexe 6 : Infomaniak et la protection de vos données personnelles

Infomaniak et la Protection de vos Données Personnelles

Disponible sur : https://www.infomaniak.com/fr/cgv/loi-sur-la-protection-des-donnees

1. Présentation de Infomaniak

Infomaniak est un prestataire suisse de services cloud et d'hébergement, reconnu pour ses engagements en matière de protection des données personnelles. Infomaniak se conforme aux normes de protection des données en vigueur, notamment au RGPD pour les clients de l'Union Européenne, et à la Loi fédérale suisse sur la protection des données (LPD).

2. Engagements de Infomaniak en matière de protection des données

Infomaniak s'engage à protéger les données personnelles de ses clients grâce à une politique de sécurité robuste et des pratiques conformes aux réglementations en vigueur. Cela inclut :

- **Transparence** : Infomaniak informe ses clients sur les types de données collectées, les finalités du traitement, et les droits des personnes concernées.
- **Sécurité** : Infomaniak met en œuvre des mesures techniques et organisationnelles pour protéger les données contre les accès non autorisés, la perte ou la divulgation.
- **Confidentialité** : Les données traitées par Infomaniak sont confidentielles et ne sont pas partagées avec des tiers sans le consentement explicite du client, sauf obligation légale.

3. Traitement des données par Infomaniak

Les données personnelles collectées par Infomaniak sont traitées dans le cadre des services fournis, tels que l'hébergement de sites web, les services cloud, et les solutions de messagerie. Infomaniak s'engage à ne traiter ces données que pour les finalités déterminées par le client.

4. Droits des personnes concernées

Les clients d'Infomaniak et les personnes concernées par les traitements de données disposent des droits suivants :

- **Droit d'accès** : Droit de savoir quelles données sont détenues par Infomaniak et comment elles sont utilisées.
- **Droit de rectification** : Droit de demander la correction de données inexactes ou incomplètes.
- **Droit à l'effacement** : Droit de demander la suppression des données personnelles, sous réserve des obligations légales.
- **Droit à la limitation du traitement** : Droit de demander la suspension du traitement des données dans certains cas.
- **Droit à la portabilité des données** : Droit de recevoir les données personnelles dans un format structuré et couramment utilisé.
- **Droit d'opposition** : Droit de s'opposer au traitement des données pour des motifs légitimes.

5. Mesures de sécurité mises en place par Infomaniak

Infomaniak utilise des technologies avancées pour sécuriser les données personnelles :

- **Chiffrement** : Les données sont chiffrées lors de leur transmission et de leur stockage.

- **Contrôles d'accès** : Accès restreint aux données, basé sur des autorisations spécifiques.
- **Surveillance** : Systèmes de détection d'intrusion et de surveillance pour prévenir et détecter les incidents de sécurité.

6. Transferts internationaux de données

Les données hébergées par Infomaniak sont principalement stockées en Suisse, un pays reconnu par l'Union Européenne comme offrant un niveau de protection des données adéquat. Infomaniak ne transfère pas de données personnelles en dehors de la Suisse ou de l'EEE sans s'assurer que des garanties appropriées sont en place.

7. Politique de rétention des données

Infomaniak conserve les données personnelles aussi longtemps que nécessaire pour les finalités pour lesquelles elles ont été collectées, conformément aux obligations légales. À la fin de cette période, les données sont supprimées ou anonymisées de manière sécurisée.

8. Contact et réclamations

Pour toute question concernant la protection des données personnelles ou pour exercer leurs droits, les clients peuvent contacter Infomaniak à l'adresse suivante :

- **Site web** : https://www.infomaniak.com/fr/support
- **Adresse** : Rue Eugène-Marziano 25, 1227 Les Acacias, Suisse
- **Téléphone** : +41 22 820 35 44

Si les clients estiment que leurs droits n'ont pas été respectés, ils peuvent introduire une réclamation auprès de l'autorité compétente, en Suisse ou auprès de la CNIL pour les résidents de l'UE.
Cette annexe résume les engagements d'Infomaniak en matière de protection des données personnelles, tels qu'ils sont décrits dans la documentation officielle disponible sur leur site internet. Les clients de Prospectia qui utilisent les services d'Infomaniak peuvent ainsi être assurés que leurs données sont traitées avec le plus grand soin et dans le respect des réglementations en vigueur.