Accord de Traitement des Données

Accord sur le traitement des données personnelles pour le compte d'un responsable du traitement conformément à l'Art. 28 du RGPD

entre le client (ci-après dénommé "Client") et CA Customer Alliance GmbH, Hausvogteipl. 12, 10117 Berlin, Allemagne (ci-après dénommé "Fournisseur").

Veuillez envoyer toute question ou commentaire concernant cet accord de traitement des données ou la protection des données en général à l'adresse e-mail suivante : dataprotection@customer-alliance.com

1. **Objet de l'Accord**

Dans le cadre de la fourniture de services conformément à l'accord de service (ci-après dénommé "Accord Principal"), il est nécessaire que le Fournisseur traite des données personnelles pour lesquelles le Client agit en tant que responsable du traitement au sens de la législation sur la protection des données (ci-après dénommées "Données du Client"). Cet accord précise les obligations et les droits des parties en matière de protection des données en relation avec l'utilisation des Données du Client par le Fournisseur pour fournir les services dans le cadre de l'Accord Principal.

2. **Portée de la mission**
    1. **Le Fournisseur traite les Données du Client pour le compte et conformément aux instructions du Client au sens de l'Art. 28 du RGPD (Traitement pour le compte). Le Client reste le responsable du traitement au sens de la législation sur la protection des données.**
    2. **Le traitement des Données du Client par le Fournisseur s'effectue de la manière, dans l'étendue et aux fins déterminées à l'Annexe 1 du présent accord ; le traitement concerne les types de données personnelles et les catégories de personnes concernées qui y sont spécifiées. La durée du traitement correspond à la durée de l'Accord Principal.**
    3. **Le traitement des Données du Client par le Fournisseur a lieu en principe à l'intérieur de l'Union européenne ou d'un autre État contractant de l'Espace économique européen (EEE). Le Fournisseur est néanmoins autorisé à traiter les Données du Client conformément aux dispositions du présent accord en dehors de l'EEE s'il informe préalablement le Client du lieu de traitement des données et si les exigences des Art. 44 à 48 du RGPD sont remplies ou si une exception selon l'Art. 49 du RGPD s'applique.**
3. **Droit du Client de donner des instructions**
    1. **Le Fournisseur traite les Données du Client conformément aux instructions du Client, à moins que le Fournisseur ne soit légalement tenu d'agir autrement. Dans ce dernier cas, le Fournisseur informe le Client de cette exigence légale avant le traitement, à moins que cette loi n'interdise cette information pour des raisons importantes d'intérêt public.**
    2. **Les instructions du Client sont en principe définitivement stipulées et documentées dans les dispositions du présent accord. Les instructions individuelles qui s'écartent des stipulations du présent accord ou qui imposent des exigences supplémentaires nécessitent un accord mutuel et doivent être faites par écrit.**
    3. **Le Fournisseur s'assure que les Données du Client sont traitées conformément aux instructions données par le Client. Si le Fournisseur est d'avis qu'une instruction donnée par le Client enfreint le présent accord ou la loi applicable sur la protection des données, il est, après en avoir informé le Client, en droit de suspendre l'exécution de l'instruction jusqu'à ce que le Client confirme l'instruction.**
4. **Responsabilité Juridique du Client**
    1. **Le Client est seul responsable de la licéité du traitement des Données du Client et de la sauvegarde des droits des personnes concernées dans la relation entre les parties.**

2. **Le Client est responsable de fournir au Fournisseur les Données du Client en temps utile pour la fourniture des services selon l'Accord Principal et il est responsable de la qualité des Données du Client. Le Client informera le Fournisseur immédiatement et complètement si, lors de l'examen des résultats du Fournisseur, il constate des erreurs ou des irrégularités concernant les dispositions de protection des données ou ses instructions.**
3. **Si le Fournisseur est tenu de fournir des informations à un organisme gouvernemental ou à une personne sur le traitement des Données du Client ou de coopérer avec ces organismes de toute autre manière, le Client est obligé, à la première demande, d'aider le Fournisseur à fournir ces informations et à remplir d'autres obligations de coopération.**

5. **Exigences pour le personnel**

Le Fournisseur engage toutes les personnes impliquées dans le traitement des Données du Client à la confidentialité en ce qui concerne le traitement des Données du Client.

6. **Sécurité du traitement**
    1. **Le Fournisseur prend, conformément à l'Art. 32 du RGPD, les mesures techniques et organisationnelles nécessaires et appropriées, en tenant compte de l'état de la technique, des coûts de mise en œuvre et de la nature, de la portée, des circonstances et des finalités des Données du Client, ainsi que des différentes probabilités et gravités du risque pour les droits et libertés des personnes concernées, afin d'assurer un niveau de protection des Données du Client adapté au risque. Les mesures actuelles se trouvent à l'Annexe 2.**
    2. **Le Fournisseur a le droit de modifier les mesures techniques et organisationnelles pendant la durée de l'accord, tant qu'elles continuent à se conformer aux exigences légales.**
7. **Engagement de sous-traitants ultérieurs**
    1. **Le Client accorde au Fournisseur l'autorisation générale d'engager d'autres sous-traitants en ce qui concerne le traitement des Données du Client. Les autres sous-traitants consultés au moment de la conclusion de l'accord figurent à l'Annexe 3. En général, aucune autorisation n'est requise pour les relations contractuelles avec des prestataires de services qui concernent l'examen ou la maintenance des procédures ou systèmes de traitement de données par des tiers ou qui impliquent d'autres services supplémentaires, même si l'accès aux Données du Client ne peut être exclu, tant que le Fournisseur prend des mesures raisonnables pour protéger la confidentialité des Données du Client.**
    2. **Le Fournisseur informera le Client de tout changement prévu concernant la consultation ou le remplacement d'autres sous-traitants. Dans des cas individuels, le Client a le droit de s'opposer à l'engagement d'un sous-traitant potentiel supplémentaire. Une objection ne peut être soulevée par le Client que pour des raisons importantes qui doivent être prouvées au Fournisseur. Dans la mesure où le Client ne s'oppose pas dans les 14 jours suivant la réception de la notification, son droit de s'opposer à l'engagement correspondant expire. Si le Client s'oppose, le Fournisseur est en droit de résilier l'Accord Principal et le présent accord avec un préavis de trois (3) mois.**
    3. **L'accord entre le Fournisseur et le sous-traitant ultérieur doit imposer à ce dernier les mêmes obligations que celles qui incombent au Fournisseur en vertu du présent accord. Les parties conviennent que cette exigence est remplie si le contrat a un niveau de protection correspondant à cet accord, respectivement si les obligations énoncées à l'Art. 28 para. 3 du RGPD sont imposées au sous-traitant ultérieur.**
8. **Droits des personnes concernées**
    1. **Le Fournisseur aide le Client, dans la mesure du raisonnable, en vertu de mesures techniques et organisationnelles à remplir l' obligation de ce dernier de répondre aux demandes d'exercice des droits des personnes concernées.**
    2. **Dans la mesure où une personne concernée soumet une demande d'exercice de ses**

droits directement au Fournisseur, le Fournisseur transmettra cette demande au Client en temps utile.

3. **Le Fournisseur informera le Client de toute information relative aux Données du Client stockées, sur les destinataires des Données du Client auxquels le Fournisseur doit les divulguer conformément à l'instruction et sur la finalité du stockage, dans la mesure où le Client ne dispose pas de ces informations et dans la mesure où il n'est pas en mesure de les recueillir lui-même.**
4. **Le Fournisseur, dans les limites de ce qui est raisonnable et nécessaire, permet au Client de corriger, supprimer ou restreindre le traitement ultérieur des Données du Client, ou à l'instruction du Client corrige, bloque ou restreint lui-même le traitement ultérieur, si et dans la mesure où cela est impossible pour le Client.**

9. **Obligations de notification et de soutien du Fournisseur**
   1. **Dans la mesure où le Client est soumis à une obligation légale de notification en raison d'une violation de la sécurité des Données du Client (en particulier conformément aux Art. 33, 34 du RGPD), le Fournisseur informera le Client en temps utile de tout événement à signaler dans son domaine de responsabilité. Le Fournisseur aidera le Client à remplir les obligations de notification à la demande de ce dernier dans la mesure raisonnable et nécessaire.**
   2. **Le Fournisseur aidera le Client dans la mesure raisonnable et nécessaire pour les analyses d'impact relatives à la protection des données à effectuer par le Client et, si nécessaire, les consultations ultérieures avec l'autorité de contrôle conformément aux Art. 35, 36 du RGPD.**
10. **Suppression des Données du Client**
    1. **Le Fournisseur supprimera les Données du Client à la fin du présent accord, à moins que le Fournisseur ne soit légalement obligé de continuer à stocker les Données du Client.**
    2. **Le Fournisseur peut conserver la documentation qui sert de preuve du traitement ordonné et précis des Données du Client, même après la fin de l'accord.**
11. **Preuves et audits**
    1. **Le Fournisseur fournira au Client, à la demande de ce dernier, toutes les informations requises et disponibles pour le Fournisseur pour prouver la conformité à ses obligations en vertu du présent accord.**
    2. **Le Client aura le droit d'auditer le Fournisseur en ce qui concerne la conformité aux dispositions du présent accord, en particulier la mise en œuvre des mesures techniques et organisationnelles ; y compris les inspections.**
    3. **Pour effectuer des inspections conformément à la Section 11.2, le Client est autorisé à accéder aux locaux commerciaux du Fournisseur dans lesquels les Données du Client sont traitées pendant les heures normales de bureau (du lundi au vendredi de 10h à 18h) après notification préalable en temps utile conformément à la Section 11.5. à ses propres frais, sans perturber le cours des affaires et sous stricte confidentialité des secrets commerciaux du Fournisseur.**
    4. **Le Fournisseur est en droit, à sa discrétion et en tenant compte des obligations légales du Client, de ne pas divulguer des informations sensibles concernant l'activité du Fournisseur ou si le Fournisseur violerait des dispositions légales ou d'autres dispositions contractuelles du fait de sa divulgation. Le Client n'est pas autorisé à accéder à des données ou informations sur les autres clients du Fournisseur, les informations sur les coûts, les rapports de contrôle de qualité et de gestion des contrats, ou toute autre donnée confidentielle du Fournisseur qui n'est pas directement pertinente pour les finalités d'audit convenues.**
    5. **Le Client informera le Fournisseur en temps utile (généralement au moins deux semaines à l'avance) de toutes les circonstances relatives à la réalisation de l'audit. Le Client peut effectuer un audit par année civile. D'autres audits sont effectués contre remboursement des coûts et après consultation avec le Fournisseur.**
    6. **Si le Client mandate un tiers pour la réalisation de l'audit, le Client obligera le tiers par écrit de la même manière que le Client est obligé vis-à-vis du Fournisseur selon cette Section 11 du présent accord. En outre, le Client obligera le tiers à maintenir le secret**

et la confidentialité, à moins que le tiers ne soit soumis à une obligation professionnelle de secret.

7. À la discrétion du Fournisseur, la preuve de la conformité aux obligations en vertu du présent accord peut être fournie, au lieu d'une inspection, en soumettant un avis ou rapport approprié et actuel d'une autorité indépendante (par exemple auditeur, service d'audit, délégué à la protection des données, département de sécurité informatique, auditeurs de protection des données ou auditeurs de qualité) ou une certification appropriée par un audit de sécurité informatique ou de protection des données -- par ex. selon "BSI-Grundschutz" -- ("rapport d'audit"), si le rapport d'audit permet au Client de manière appropriée de se convaincre de la conformité aux obligations contractuelles.

12. Durée du contrat et résiliation

La durée et la résiliation du présent accord sont régies par les dispositions relatives à la durée et à la résiliation de l'Accord Principal. Une résiliation de l'Accord Principal entraîne automatiquement l'annulation du présent accord. Une résiliation isolée du présent contrat est exclue.

13. Responsabilité
    1. La responsabilité du Fournisseur en vertu du présent accord est régie par les limitations de responsabilité prévues dans l'Accord Principal. Dans la mesure où des tiers font valoir des réclamations contre le Fournisseur qui sont causées par la violation fautive du présent accord ou de l'une de ses obligations en tant que responsable du traitement au sens de la législation sur la protection des données qui l'affecte, le Client doit, à la première demande, indemniser et dégager le Fournisseur de ces réclamations.
    2. Le Client s'engage à indemniser le Fournisseur à la première demande contre toutes les amendes possibles imposées au Fournisseur correspondant à la part de responsabilité du Client pour l'infraction sanctionnée par l'amende.
14. Dispositions finales
    1. Les litiges découlant du présent contrat sont régis par le droit allemand. Le lieu d'exécution et de juridiction est le siège social du Contractant. En cas de contradictions dans les deux versions linguistiques, la version allemande prévaut.
    2. Au cas où des dispositions individuelles du présent accord seraient inefficaces ou deviendraient inefficaces ou contiendraient une lacune, les dispositions restantes resteront inchangées. Les parties s'engagent à remplacer la disposition inefficace par une disposition légalement admissible qui se rapproche le plus de l'objectif de la disposition inefficace et qui satisfait ainsi aux exigences de l'Art. 28 du RGPD.
    3. En cas de conflits entre le présent accord et d'autres arrangements entre les parties, en particulier l'Accord Principal, les dispositions du présent accord prévalent.

Annexe :

Annexe 1 : Finalité, type et étendue du traitement des Données du Client, types de données personnelles et catégories de personnes concernées

Annexe 2 : Mesures techniques et organisationnelles

Annexe 3 : Sous-traitants ultérieurs

Annexe 1 - Finalité, type et étendue du traitement des Données du Client, types de données personnelles et catégories de personnes concernées

1. Finalité du traitement des données

Le Fournisseur envoie des messages aux clients finaux du Client et pour le compte du Client avant et pendant la fourniture de son service pour obtenir des retours, améliorer, standardiser et automatiser

la communication entre le Client et ses clients finaux. Les résultats sont traités et évalués pour le compte du Client. En outre, des évaluations provenant de retours indirects et dérivés, tels que des informations provenant de sources internes et/ou publiques, sont utilisées pour représenter pleinement la voix du client final. Le Fournisseur agrège et anonymise ainsi les données du Client collectées via la plateforme afin d'offrir au Client des services supplémentaires tels que des rapports, des analyses comparatives et des fonctionnalités de suivi des KPI liées aux retours donnés par les clients finaux du Client.

2. **Types de données personnelles a. Données de base (par ex. nom, sexe, langue) ; b. Données de contact (par ex. adresse e-mail, adresse, n° de téléphone) ; c. Données de communication (par ex. correspondance par e-mail) ; d. Données contractuelles (par ex. durée du contrat, informations sur la fourniture de services telles que chiffre d'affaires ou coûts) ; e. Le cas échéant, données de segmentation individuelles existantes du Client pour ses clients finaux telles que mode de conclusion du contrat (internet, téléphone, etc.), pays d'origine, catégorie de service ou groupe d'âge ; f. Évaluation du Client par le client final (avis client) ; g. Analyses de satisfaction (par ex. évaluations de texte, de sujet et d'expression).**
3. **Catégories de personnes concernées a. Personnel du Client ; b. Clients finaux du Client ; c. Fournisseurs du Client.**

Annexe 2 -- Mesures techniques et organisationnelles

Les mesures techniques et organisationnelles suivantes ont été prises pour protéger les données personnelles :

- **1. Contrôle d'accès physique**

L'accès aux équipements de traitement des données avec lesquels les données personnelles sont traitées et utilisées doit être refusé aux personnes non autorisées.

Assuré par :

a. Définition des zones de sécurité et des personnes autorisées

b. Sécurité des salles (clé, store, etc.)

c. Registre de présence

d. Sécurité extérieure du bâtiment (clôture, portes/fenêtres de sécurité)

e. Soin dans la sélection des gardes de sécurité

f. Soin dans la sélection des services de nettoyage

g. Vidéosurveillance des entrées

h. Gestion des clés / réglementation (verrouillage et déverrouillage) / documentation de l'attribution des clés

i. Système automatique de contrôle d'accès

j. Cartes à puce / systèmes de transpondeur

k. Système de verrouillage manuel

l. Serrures de sécurité

m. Portes avec bouton (extérieur)

n. Droits d'accès très restreints à la salle des serveurs

o. Serveurs dans des armoires serveurs verrouillables, clé au département informatique

2. **Contrôle d'accès (externe)**

Il faut empêcher que les systèmes de traitement des données puissent être utilisés par des personnes non autorisées.

Assuré par :

a. Verrouillabilité de la station de données

b. Connexion avec nom d'utilisateur et mot de passe et spécifications pour leur modification (période de validité max. 1 an)

c. Cryptage des mots de passe

d. Logiciel antivirus serveur

e. Logiciel antivirus clients

f. Pare-feu

g. Gestion des appareils mobiles

h. Utilisation de tunnels VPN pour l'accès à distance

i. Verrouillage des interfaces externes (USB)

j. Cryptage des ordinateurs portables / tablettes

k. Gestion des autorisations d'utilisateur

l. Création de profils d'utilisateur

m. Attribution centralisée des mots de passe

n. Politique de mot de passe sécurisé

o. Politique de suppression / destruction

p. Politique de protection des données et de sécurité

3. **Contrôle d'accès (interne)**

Il faut veiller à ce que les personnes autorisées à utiliser un système de traitement des données ne puissent accéder qu'aux données soumises à leur autorisation d'accès et que les données personnelles ne puissent être lues, copiées, modifiées ou supprimées sans autorisation pendant le traitement, l'utilisation et après le stockage.

Assuré par :

a. Authentification avec utilisateurs + mots de passe

b. Gestion des droits graduée par utilisateur / définition des rôles

c. Gestion des droits d'utilisateur par les administrateurs

d. Nombre minimum d'administrateurs

e. Documentation de la gestion des droits

f. Assombrissement de l'écran pendant les interruptions de travail

g. Mises à jour de sécurité régulières

h. Déchiqueteuse (niveau min. 3, coupe croisée)

i. Journalisation des accès aux applications, spécifiquement lors de la saisie, de la modification et de la suppression de données

j. Politique de mot de passe sécurisé

k. Politique de suppression / destruction

l. Politique de protection des données et de sécurité

4. **Contrôle de séparation**

Assurer que les données collectées à des fins différentes puissent être traitées séparément.

Assuré par :

a. Systèmes logiciels séparés

b. Bases de données et stockage séparés

c. Contrôle via concept d'autorisation

d. Séparation par règlements d'accès

e. Définition des droits de base de données

5. **Contrôle de transfert**

Il faut s'assurer que les données personnelles ne puissent pas être lues, copiées, modifiées ou supprimées sans autorisation pendant la transmission électronique ou pendant leur transport ou leur stockage sur des supports de données, et qu'il soit possible de vérifier et d'établir à quels points une transmission de données personnelles est prévue par des équipements de transmission de données.

Assuré par :

a. Détermination des pouvoirs pour le traitement des données

b. Détermination des parties autorisées à transmettre, des destinataires de la transmission et des voies de transmission

c. Sécurité du transport des supports de données

d. W-LAN sécurisé

e. Règlements sur la destruction des supports de données

f. Cryptage des e-mails (S/MIME, PGP, REDDCRYPT)

g. Politique de sécurité informatique

6. **Contrôle de saisie**

Il faut veiller à ce qu'il soit possible de vérifier et d'établir rétrospectivement si et par qui des données personnelles ont été saisies dans des systèmes de traitement des données, modifiées ou supprimées.

Assuré par :

a. Gestion des accès en lecture / écriture

b. Journalisation des accès en lecture/écriture et des appels de programme

c. Marquage des documents de saisie de données avec nom et date après saisie

d. Dispositions sur la modification des droits d'accès et de la responsabilité des données

e. Responsabilités strictes pour les suppressions

7. **Contrôle de disponibilité**

Il faut veiller à ce que les données personnelles soient protégées contre la destruction ou la perte accidentelle.

Assuré par :

a. Création de copies de sauvegarde périodiques

b. Protection UPS en cas de panne de courant

c. Protection antivirus/pare-feu

d. Plan d'urgence

e. Plan de récupération

f. Protection DDoS en permanence active

8. **Contrôle du traitement des commandes**

Il faut s'assurer que les données personnelles traitées pour le compte du client ne puissent être traitées que conformément aux instructions du client.

Assuré par :

a. Détermination des droits et obligations du contractant

b. Contrat pour le traitement des données sur commande

c. Formation de tous les employés ayant des droits d'accès

d. Audits réguliers de protection des données

e. Accord sur les droits de contrôle et d'audit

f. Le contractant nomme un délégué à la protection des données ou une personne responsable

Entreprise, Adresse	**Service/Type de traitement**	**Couverture juridique**	**Mesures pour un niveau de protection comparable (uniquement dans les pays tiers)**
ALL-INKL.COM - Neue Medien Münnich, Hauptstraße 68, 02742 Friedersdorf Allemagne	Hébergement Web	Accord de traitement des données	/
Apollon 415, rue Mission, Étage 37, San Francisco, Californie 94105, USA	Enrichissement des données	Clause contractuelle type et évaluation individuelle jusqu'à un niveau de protection comparable à la norme au sein de l'UE.	Certificat ISO (27001) et conformité SOC-2 certifiée par A-LIGN.
char desarrollo de sistemas s.l.u. Arboretum du Parc Empresarial – Avda. de la Fama, 16-20, 3ª plante 08940 Cornellà de Llobregat – Barcelone – Espagne	Fournisseur de système de gestion immobilière	Accord de traitement des données	Cryptage des données au repos et pour les données en transit - HTTPS pour tous les services utilisant TLS (SSL) et entièrement conforme au RGPD

CHARGEBEE INC., 340 S. Lemon Avenue, bureau n° 1537, noyer, CA 91789 États-Unis	Facturation	Clause contractuelle type et évaluation individuelle jusqu'à un niveau de protection comparable à la norme au sein de l'UE.	Certifications et audits tiers ; Certificat ISO 27001 ; Normes SOC 1/SOC 2 et MFA ; politiques de sécurité au niveau du réseau, des applications et des opérations ; Configuration de la sécurité AWS : plusieurs certifications pour les centres de données, notamment la conformité ISO 27001, la certification PCI et les rapports SOC.
Google SARL, 1600 Amphithéâtre Parkway, vue sur la montagne, CA 94043 États-Unis	Google WorkspaceGoogle Analytics	Clause contractuelle type et évaluation individuelle jusqu'à un niveau de protection comparable à la norme au sein de l'UE.	Certificats ISO (ISO 27001, 27017, 27018) ; Ligne directrice sur la protection des données ; Centre de conformité et rapports.
HelpScout PBC 177 Huntington Ave, Boston, MA 02115, États-Unis	Service d'assistance	Clause contractuelle type et évaluation individuelle jusqu'à un niveau de protection comparable à la norme au sein de l'UE.	Help Scout est certifié SOC2 Type 2 pour la sécurité et la disponibilité. Lois de l'UE sur la protection des données, y compris le règlement général sur la protection des données de l'UE (« RGPD UE ») Configuration de la sécurité AWS

Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen Allemagne	Hébergement	Accord de traitement des données	/
HubSpot, Inc., 25 First Street, Cambridge, MA 02141 États-Unis	Inbound-Marketing, ventes, réussite client et gestion de la relation client	Clause contractuelle type et évaluation individuelle jusqu'à un niveau de protection comparable à la norme au sein de l'UE.	Règles d'entreprise contraignantes ; Data Center (certificat ISO 27001 / audit SOC 2) ; Cryptage HTTP.
Luzmo SA Tiensevest 102 case 201, B-3000 Louvain, Belgique	Analyse conversationnelle	#VALUE!	Conforme AICPA SOC 2 Type II
Mailgun Technologies, Inc., 548 Market Street, Suite 43099, San Francisco, CA 94101 États-Unis	Fournisseur de messagerie (e-mail-API)	Clause contractuelle type et évaluation individuelle jusqu'à un niveau de protection comparable à la norme au sein de l'UE.	Analyse du réseau externe et test d'intrusion ; cryptage des données ; détection d'intrusion; procédure de gestion des fournisseurs - contrôle et audit fréquent de tous les sous-traitants.
Société Microsoft One Microsoft Way Redmond, WA 98052-6399 USA	Bureau 365	Clause contractuelle type et évaluation individuelle jusqu'à un niveau de protection comparable à la norme au sein de l'UE.	Rapports de confiance et d'audit externes ; ISO 27001, 27017, 27018, 22301, 277701 certificats; politique de prévention des pertes de données ; Conforme aux normes SSAE 18 SOC 1 Type II et SSAE 18 SOC 2 Type II.

Nonius Rua Eng.º Frederico Ulrich, 2650 4470-605 Moreira da Maia Portugal	Fournisseur de système de gestion immobilière	Accord de traitement des données	Cryptage des données au repos et pour les données en transit - HTTPS pour tous les services utilisant TLS (SSL) et entièrement conforme au RGPD
OpenAI OpCo, LLC 3180 18th Street, San Francisco, CA 94110	Informations, rapports, analyses	Accord de traitement des données	/
OVH GmbH, Rue Saint-Johanner 41-43, 66111 Sarrebruck Allemagne	Hébergement	Accord de traitement des données	/
Scaling Technologies GmbH, Pfarrer-Hillmann-Weg 1, 51069 Cologne Allemagne	Opérations Web	Accord de traitement des données	/

Stripe, Inc. 510, rue Townsend, San Francisco, CA 94103 États-Unis	Solution de paiement	Clause contractuelle type et évaluation individuelle jusqu'à un niveau de protection comparable à la norme au sein de l'UE.	Cryptage des données au repos et pour les données en transit - HTTPS pour tous les services utilisant TLS (SSL) ; tous les numéros de carte sont cryptés au repos avec AES-256 ; journaux d'audit ; politique de gestion des accès ; Certificat de fournisseur de services PCI niveau 1.

Twilio, Inc., 375, rue Beale, Suite 300, San Francisco, Californie 94105 États-Unis	Fournisseur de messages courts (SMS)	Clause contractuelle type et évaluation individuelle jusqu'à un niveau de protection comparable à la norme au sein de l'UE.	Règles d'entreprise contraignantes ; cadre de sécurité basé sur la norme ISO 27001 ; ISO/CEI 27001, ISO/CEI 27017 et 27018, SOC 2 Type II, PCI DSS niveau 1 certificats; Configuration de la sécurité AWS : plusieurs certifications pour les centres de données, notamment la conformité ISO 27001, la certification PCI et le rapport SOC ; les bases de données (données client) sont cryptées à l'aide de la norme Advanced Encryption Standard et les données client sont cryptées lorsqu'elles transitent entre l'application logicielle du client et les services à l'aide de TLS v1.2 ; tests d'intrusion ; politiques et procédures de gestion des incidents de sécurité conformément à la norme NIST SP 800-61.