La version originale cet Accord de Traitement des Données a été rédigée en anglais, puis traduite dans d'autres langues. Ces traductions internes sont fournies uniquement par courtoisie et n'ont aucune valeur juridique.

Accord de Traitement des Données

Accord sur le traitement de données personnelles pour le compte d'un responsable de traitement conformément à l'art. 28 du RGPD entre le client (ci-après dénommé "**Client**") et CA Customer Alliance GmbH, Ullsteinstr. 130, 12109 Berlin, Allemagne (ci-après dénommé "**Fournisseur**").

1. Objet de l'accord

Dans le cadre de la prestation de services telle que prévue par 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 de traitement au sens de la législation sur la protection des données (ci-après dénommées "**Données du Client**"). Cet accord précise les obligations en matière de protection des données et les droits des parties en ce qui concerne l'utilisation par le Fournisseur des Données du Client pour la prestation des services en vertu de l'Accord Principal.

2. Portée de la commission

2.1. Le Fournisseur traitera les Données du Client au nom et conformément aux instructions du Client au sens de l'art. 28 du RGPD (Traitement pour le compte). Le Client reste le responsable de traitement en matière de protection des données.

2.2. Le traitement des Données du Client par le Fournisseur se fait de la manière, dans la mesure et aux fins déterminées dans l'**Annexe 1** à cet accord ; le traitement concerne les types de données personnelles et les catégories de personnes concernées spécifiées dans ladite annexe. La durée du traitement correspond à la durée de l'Accord Principal.

2.3. Le traitement des Données du Client par le Fournisseur se déroulera en principe à l'intérieur de l'Union européenne ou d'un autre État contractant de l'Espace économique européen (EEE). Néanmoins, le Fournisseur est 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 de l'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

3.1. Le Fournisseur traite les Données du Client conformément aux instructions du Client, sauf si le Fournisseur est légalement tenu de faire autrement. Dans ce dernier cas, le Fournisseur informera le Client de cette obligation légale avant le traitement, sauf si la loi interdit une telle information pour des motifs importants d'intérêt public.

3.2. Les instructions du Client sont en principe définitivement stipulées et documentées dans les dispositions du présent accord. Les instructions individuelles qui dérogent aux stipulations

du présent accord ou qui imposent des exigences supplémentaires nécessitent un accord mutuel et doivent être formulées par écrit.

3.3. Le Fournisseur veillera à ce que les Données du Client soient 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 législation applicable en matière de protection des données, il est en droit, après avoir informé le Client en conséquence, de suspendre l'exécution de l'instruction jusqu'à ce que le Client confirme l'instruction.

4. Responsabilité légale du Client

4.1. Le Client est seul responsable de la licéité du traitement des Données du Client et de la protection des droits des personnes concernées dans la relation entre les parties.

4.2. Le Client est responsable de fournir au Fournisseur les Données du Client en temps utile pour la prestation des services conformément à l'Accord Principal, et il est responsable de la qualité des Données du Client. Le Client informera immédiatement et intégralement le Fournisseur s'il constate des erreurs ou des irrégularités lors de l'examen des résultats du Fournisseur concernant les dispositions en matière de protection des données ou ses instructions.

4.3. Si le Fournisseur est tenu de fournir des informations à une autorité gouvernementale ou à une personne concernant le traitement des Données du Client ou de coopérer de quelque manière que ce soit avec ces organismes, le Client est tenu, sur première demande, d'assister le Fournisseur dans la fourniture de telles informations et dans l'accomplissement d'autres obligations de coopération.

5. Exigences relatives au personnel

Le Fournisseur s'engage à imposer à toutes les personnes impliquées dans le traitement des Données du Client une obligation de confidentialité à l'égard du traitement des Données du Client.

6. Sécurité du traitement

6.1. 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 l'art, 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 probabilités et de la gravité différentes des risques pour les droits et libertés des personnes concernées, afin d'assurer un niveau de protection des Données du Client approprié au risque. Les mesures actuelles se trouvent en **Annexe 2**.

6.2. Le Fournisseur a le droit de modifier les mesures techniques et organisationnelles pendant la durée de l'accord, tant qu'elles continuent de répondre aux exigences légales.

7. Engagement de sous-traitants supplémentaires

7.1. Le Client accorde au Fournisseur l'autorisation générale d'engager des sous-traitants supplémentaires pour le traitement des Données du Client. Les sous-traitants

supplémentaires consultés au moment de la conclusion de l'accord sont indiqués à l'**Annexe 3**. En général, aucune autorisation n'est requise pour les relations contractuelles avec les prestataires de services qui sont chargés de l'examen ou de la maintenance des procédures ou des systèmes de traitement des données par des tiers ou qui impliquent d'autres services supplémentaires, même si l'accès aux Données du Client ne peut pas être exclu, tant que le Fournisseur prend des mesures raisonnables pour protéger la confidentialité des Données du Client.

7.2. Le Fournisseur informera le Client de toute modification envisagée concernant la consultation ou le remplacement des sous-traitants supplémentaires. Dans des cas individuels, le Client a le droit de s'opposer à l'engagement éventuel d'un sous-traitant supplémentaire. Une objection ne peut être formulée par le Client que pour des raisons importantes qui doivent être prouvées au Fournisseur. Dans la mesure où le Client n'exprime pas d'objection 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.

7.3. L'accord entre le Fournisseur et le sous-traitant supplémentaire doit imposer à ce dernier les mêmes obligations que celles incombant au Fournisseur en vertu du présent accord. Les parties conviennent que cette exigence est remplie si le contrat offre un niveau de protection correspondant à celui du présent accord, respectivement si les obligations énoncées à l'art. 28, par. 3, du RGPD sont imposées au sous-traitant supplémentaire.

8. Droits des personnes concernées

8.1. Le Fournisseur assistera le Client dans la mesure du raisonnable au moyen de mesures techniques et organisationnelles pour répondre aux demandes d'exercice des droits des personnes concernées.

8.2. Dans la mesure où une personne concernée soumet une demande d'exercice de ses droits directement au Fournisseur, ce dernier transmettra cette demande au Client en temps utile.

8.3. Le Fournisseur informera le Client de toute information concernant les Données du Client stockées, les destinataires des Données du Client auxquels le Fournisseur devra les divulguer conformément à l'instruction et la finalité du stockage, dans la mesure où le Client n'a pas cette information à sa disposition et qu'il n'est pas en mesure de la collecter lui-même.

8.4. Le Fournisseur permettra, dans les limites du raisonnable et du nécessaire, au Client de corriger, supprimer ou restreindre le traitement ultérieur des Données du Client, ou, sur instruction du Client, de corriger, bloquer ou restreindre le traitement ultérieur lui-même, dans la mesure où cela est impossible pour le Client.

9. Obligations de notification et de soutien du Fournisseur

9.1. Dans la mesure où le Client est soumis à une obligation légale de notification en cas de violation de la sécurité des Données du Client (en particulier en vertu de l'art. 33 et 34 du RGPD), le Fournisseur informera le Client en temps utile de tout événement à signaler

relevant de sa responsabilité. Le Fournisseur assistera le Client dans l'accomplissement des obligations de notification à la demande de ce dernier, dans la mesure du raisonnable et du nécessaire.

9.2. Le Fournisseur assistera le Client dans la mesure du raisonnable et du nécessaire pour les évaluations d'impact relatives à la protection des données à effectuer par le Client et, le cas échéant, pour les consultations ultérieures avec l'autorité de contrôle conformément à l'art. 35 et 36 du RGPD.

10. Suppression des Données du Client

10.1. Le Fournisseur supprimera les Données du Client à la résiliation du présent accord, sauf si le Fournisseur est légalement tenu de conserver les Données du Client.

10.2. Le Fournisseur peut conserver la documentation servant de preuve du traitement ordonné et exact des Données du Client, même après la résiliation de l'accord.

11. Preuves et audits

11.1. Le Fournisseur fournira au Client, à la demande de ce dernier, toutes les informations nécessaires et disponibles au Fournisseur pour prouver le respect de ses obligations en vertu du présent accord.

11.2. Le Client est autorisé à auditer le Fournisseur en ce qui concerne le respect des dispositions du présent accord, en particulier la mise en œuvre des mesures techniques et organisationnelles, y compris les inspections.

11.3. 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 de travail habituelles (du lundi au vendredi de 10h00 à 18h00) après notification préalable en conformité avec la Section 11.5, à ses propres frais, sans perturbation du déroulement des activités commerciales et dans le strict respect des secrets d'entreprise et commerciaux du Fournisseur.

11.4. Le Fournisseur est en droit, à sa discrétion et en tenant compte des obligations légales du Client, de ne pas divulguer d'informations sensibles concernant les activités du Fournisseur ou si la divulgation serait contraire aux dispositions légales ou contractuelles en raison de sa divulgation. Le Client n'a pas le droit d'accéder aux données ou aux informations concernant les autres clients du Fournisseur, les informations sur les coûts, les rapports de contrôle de la 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.

11.5. Le Client informera le Fournisseur en temps utile (généralement au moins deux semaines à l'avance) de toutes les circonstances liées à la réalisation de l'audit. Le Client peut effectuer un audit par an. Les audits ultérieurs sont effectués moyennant remboursement des frais et après consultation avec le Fournisseur.

11.6. Si le Client mandate un tiers pour effectuer l'audit, le Client doit lier le tiers par écrit de la même manière que le Client est lié vis-à-vis du Fournisseur conformément à cette Section 11

du présent accord. De plus, le Client doit imposer au tiers l'obligation de maintenir le secret et la confidentialité, sauf si le tiers est soumis à une obligation professionnelle de secret.

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

12. Durée et résiliation du contrat

La durée et la résiliation du présent accord seront régies par les dispositions de durée et de 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

13.1. La responsabilité du Fournisseur en vertu du présent accord sera régie par les limitations de responsabilité prévues dans l'Accord Principal. Dans la mesure où des tiers font valoir des droits contre le Fournisseur qui sont causés par la violation par le Client de son obligation de ce fait que le Client est le responsable de traitement en matière de protection des données, le Client doit, sur première demande, indemniser et dégager le Fournisseur de ces demandes.

13.2. Le Client s'engage à indemniser le Fournisseur sur première demande contre toutes les amendes éventuelles imposées au Fournisseur correspondant à la part de responsabilité du Client dans l'infraction sanctionnée par l'amende.

14. Dispositions finales

14.1. Les litiges découlant de ce contrat seront régis par le droit allemand. Le lieu d'exécution et de juridiction sera le siège social de l'Entrepreneur. En cas de contradictions entre les deux versions linguistiques, la version allemande prévaudra.

14.2. En cas de dispositions individuelles de cet accord qui seraient inefficaces ou deviendraient inefficaces ou contiendraient une lacune, les dispositions restantes demeureront inchangées. Les parties s'engagent à remplacer la disposition inefficace par une disposition légalement admissible qui se rapproche le plus de l'objet de la disposition inefficace et qui satisfait ainsi aux exigences de l'art. 28 du RGPD.

14.3. En cas de conflit entre le présent accord et d'autres accords entre les parties, en particulier l'Accord Principal, les dispositions du présent accord prévaudront.

Annexe :

Annexe 1 : Objectif, 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 supplémentaires

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

1. Objectif du traitement des données

Le Fournisseur envoie des messages aux clients finaux au nom du Client avant et pendant la fourniture de son service afin d'obtenir des commentaires, d'améliorer, de normaliser et d'automatiser la communication entre le Client et ses clients finaux. Les résultats sont traités et évalués au nom du Client. De plus, les évaluations des commentaires indirects et dérivés, tels que les informations provenant de sources internes et/ou publiques, sont utilisées pour représenter pleinement la voix du client final. Le Fournisseur agrège ainsi et anonymise les données du Client collectées par le biais de la plateforme afin d'offrir au Client des services supplémentaires tels que des rapports, des comparaisons et des fonctionnalités de surveillance des KPI liées aux commentaires donnés par les clients finaux du Client.

2. Types de données personnelles

a) Données de base (par exemple, nom, genre, langue) ;
b) Données de contact (par exemple, adresse e-mail, adresse, numéro de téléphone) ;
c) Données de communication (par exemple, correspondance par e-mail) ;
d) Données contractuelles (par exemple, durée du contrat, informations sur la prestation de services telles que le chiffre d'affaires ou les coûts) ;
e) Si applicable, données de segmentation individuelle existantes du Client pour ses clients finaux, telles que la manière de conclure le contrat (internet, téléphone, etc.), pays d'origine, catégorie de service ou groupe d'âge ;
f) Évaluation du Client par le client final (avis du client) ;
g) Analyses de satisfaction (par exemple, évaluations de texte, de sujets et d'expressions).

3. Catégories de personnes concernées

a) Personnel du Client ;
b) Clients finaux du Client ;
c) Fournisseur 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'entrée

L'accès aux équipements de traitement des données traitant les données personnelles sera refusé aux personnes non autorisées.

Assuré par :

a) Définition des zones de sécurité et des personnes autorisées
b) Sécurité des locaux (clé, volet roulant, etc.)
c) Registre de présence
d) Sécurité extérieure du bâtiment (clôture, portes/fenêtres de sécurité)
e) Sélection soignée des agents de sécurité
f) Sélection soignée des services de nettoyage
g) Vidéosurveillance des entrées
h) Gestion des clés / documentation de l'attribution des clés
i) Système de contrôle d'accès automatique
j) Cartes à puce / systèmes de transpondeur
k) Système de verrouillage manuel
l) Serrures de sécurité
m) Portes avec poignée (à l'extérieur)

2. Contrôle d'accès (externe)

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

Assuré par :

a) Verrouillage de la station de données
b) Connexion avec nom d'utilisateur et mot de passe et spécifications pour leur modification
c) Chiffrement des mots de passe
d) Serveur de logiciel anti-virus
e) Clients de logiciel anti-virus
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) Chiffrement des ordinateurs portables / tablettes
k) Gestion des autorisations des utilisateurs
l) Création de profils d'utilisateurs
m) Attribution centralisée de 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 convient de veiller à ce que les personnes autorisées à utiliser un système de traitement des données ne puissent accéder qu'aux données auxquelles elles sont autorisées à accéder et que les données personnelles ne puissent pas être lues, copiées, modifiées ou supprimées sans autorisation pendant le traitement, l'utilisation et après le stockage.

Assuré par :

a) Gestion des droits spécifiques à l'utilisateur
b) Gestion des droits de l'utilisateur par les administrateurs
c) Minimum d'administrateurs
d) Documentation de la gestion des droits
e) Assombrissement de l'écran lors des interruptions de travail
f) Mises à jour de sécurité régulières
g) Destructeur (niveau de sécurité minimum 3, coupe croisée)
h) Enregistrement des accès aux applications, en particulier lors de l'entrée, de la modification et de la suppression de données

4. Contrôle de séparation

Il convient de garantir 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 un concept d'autorisation
d) Séparation par le biais de règles d'accès
e) Définition des droits de la base de données

5. Contrôle des transferts

Il convient de veiller à ce que les données personnelles ne puissent pas être lues, copiées, modifiées ou supprimées sans autorisation lors de la transmission électronique ou lors de leur transport ou 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 l'équipement 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 autorisées
c) Sécurité du transport des supports de données
d) Sécurité du réseau local sans fil (W-LAN)
e) Règlements sur la destruction des supports de données
f) Chiffrement

6. Contrôle de la saisie

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

Assuré par :

a) Gestion de l'accès en lecture/écriture
b) Enregistrement des accès en lecture/écriture et des appels de programmes
c) Marquage des documents de saisie de données avec le nom et la date après la saisie
d) Dispositions sur la modification des droits d'accès et de la responsabilité des données
e) Responsabilités claires en ce qui concerne les suppressions

7. Contrôle de la disponibilité

Il convient de 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 par UPS en cas de panne de courant
c) Protection antivirus/pare-feu
d) Plan d'urgence
e) Plan de reprise
f) Protection DDoS en permanence active

8. Contrôle du traitement des commandes

Il convient de veiller à ce 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 des obligations du prestataire
b) Contrat de traitement des données commissionné
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.

Annexe 3 – Sous-traitants supplémentaires			
Entreprise, Adresse	**Service / Type de Traitement**	**Couverture Légale**	**Mesures pour un Niveau de Protection Comparable (uniquement dans les Pays Tiers)**
ALL-INKL.COM - Neue Medien Münnich, Hauptstraße 68, 02742 Friedersdorf Germany	Hébergement web	Accord de traitement de données	/
CHARGEBEE INC., 340 S. Lemon Avenue, Suite #1537, Walnut, CA 91789 USA	Facturation	Clause contractuelle standard et évaluation individuelle à un niveau de protection comparable à celui des normes au sein de l'UE.	Certifications et audits de tiers ; certificat ISO 27001 ; normes SOC 1/SOC 2 et MFA ; politiques de sécurité au niveau du réseau, de l'application et des opérations ; configuration de sécurité AWS - plusieurs certifications pour les centres de données, notamment la conformité ISO 27001, la certification PCI et les rapports SOC.
Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043 USA	Google Workspace Google Analytics	Clause contractuelle standard et évaluation individuelle à un niveau de protection comparable à celui des normes au sein de l'UE.	Certificats ISO (ISO 27001, 27017, 27018) ; Directive sur la protection des données ; Centre de conformité et rapports.
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen Germany	Hébergement	Accord de traitement de données	/
HubSpot, Inc., 25 First Street, Cambridge, MA 02141 USA	Marketing entrant et ventes	Clause contractuelle standard et évaluation individuelle à un niveau de protection comparable à celui des normes au sein de l'UE.	Règles d'entreprise contraignantes ; Centre de données (certificat ISO 27001 / audit SOC 2) ; chiffrement HTTPs.

Intercom, Inc., 55 2nd Street, 4th Fl., San Francisco, CA 94105 USA	Chat en direct	Clause contractuelle standard et évaluation individuelle à un niveau de protection comparable à celui des normes au sein de l'UE.	Audits externes, tests d'intrusion et primes de bogues ; audit SOC 2 ; certificat ISO 27001 ; audit HIPAA ; configuration de sécurité AWS ; les API et les points de terminaison des applications sont uniquement en TLS/SSL ; politique de sécurité ; formation à la sécurité et à la sensibilisation.
Impala Travel Technology Ltd., 70 White Lion Street, London, N1 9PP UK	Extraction de données du PMS (API)	Accord de traitement de données	Protection adéquate des données personnelles au Royaume-Uni - Décision d'exécution de la Commission européenne du 28 juin 2021 - C(2021) 4800.
Mailgun Technologies, Inc., 548 Market Street, Suite 43099, San Francisco, CA 94101 USA	Fournisseur de messagerie électronique (API e-mail)	Clause contractuelle standard et évaluation individuelle à un niveau de protection comparable à celui des normes au sein de l'UE.	Scan et test de pénétration du réseau externe ; chiffrement des données ; détection des intrusions ; procédure de gestion des fournisseurs - contrôle et audits fréquents de tous les sous-traitants.
Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA	Office 365	Clause contractuelle standard et évaluation individuelle à un niveau de protection comparable à celui des normes au sein de l'UE.	Rapports externes de confiance et d'audit ; certificats ISO 27001, 27017, 27018, 22301, 277701 ; politique de prévention des pertes de données ; conformité SSAE 18 SOC 1 de type II et SSAE 18 SOC 2 de type II.
OVH GmbH, St. Johanner Str. 41-43, 66111 Saarbrücken Germany	Hébergement	Accord de traitement de données	/
Scaling Technologies GmbH, Pfarrer-Hillmann-Weg 1, 51069 Köln Germany	Opérations Web	Accord de traitement de données	/

Stripe, Inc. 510 Townsend Street San Francisco, CA 94103 USA	Solution de paiement	Clause contractuelle standard et évaluation individuelle à un niveau de protection comparable à celui des normes au sein de l'UE.	Chiffrement des données au repos et des données en transit - HTTPS pour tous les services utilisant TLS (SSL) ; tous les numéros de carte sont chiffrés au repos avec AES-256 ; journaux d'audit ; politique de gestion des accès ; certificat de Prestataire de Services PCI de Niveau 1.
SugarCRM, Inc., 10050 N Wolfe Road, SW2-130 Cupertino, CA 95014 USA	Gestion de la relation client	Clause contractuelle standard et évaluation individuelle à un niveau de protection comparable à celui des normes au sein de l'UE.	Certificat SOC II ; chiffrement pour tous les mots de passe, données clés et sauvegardes ; toutes les données de production et des clients sont chiffrées en transit et au repos ; authentification multifacteur ; outils de prévention des pertes de données ; hébergé en Irlande (UE) ; configuration de sécurité AWS - plusieurs certifications pour les centres de données, notamment la conformité ISO 27001, la certification PCI et les rapports SOC.
Twilio, Inc., 375 Beale Street, Suite 300, San Francisco, CA 94105 USA	Fournisseur de messages courts (SMS)	Clause contractuelle standard et évaluation individuelle à un niveau de protection comparable à celui des normes au sein de l'UE.	Règles d'entreprise contraignantes ; cadre de sécurité basé sur ISO 27001 ; certificats ISO/IEC 27001, ISO/IEC 27017 et 27018, SOC 2 de type II, niveau 1 de la norme PCI DSS ; configuration de sécurité AWS - plusieurs certifications pour les centres de données, notamment la conformité à ISO 27001, la certification PCI et le rapport SOC ; les bases de données (données clients) sont chiffrées à l'aide de l'Advanced Encryption Standard, et les données clients sont chiffrées lorsqu'elles transitent entre l'application logicielle du client et les services à l'aide de TLS v1.2 ; tests de pénétration ; politiques et procédures de gestion des incidents de sécurité conformes à NIST SP 800-61.