Accord relatif au traitement des données (version 1.2)

Entre

Le CLIENT (le sous-traitant)

et

« Tjekvik »

Autoinnovation ApS
Kronprinsessegade 6
1306 Copenhague K Danemark
TVA : DK37211192
(+45) 3070 6970
admin@tjekvik.com

(le sous-traitant)

chacun étant une « partie » ; conjointement, « les parties »

ONT CONVENU des Clauses contractuelles suivantes (les Clauses) afin de satisfaire aux exigences du RGPD et de garantir la protection des droits de la personne concernée.

1. PRÉAMBULE

1.1. Les présentes Clauses contractuelles (les Clauses) définissent les droits et obligations du responsable du traitement et du sous-traitant lorsqu'ils traitent des données à caractère personnel pour le compte du responsable du traitement.

1.2. Les Clauses ont été conçues pour assurer le respect par les parties de l'article 28(3) du Règlement 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, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données).

1.3. Dans le cadre de la fourniture de « Tjekvik, réception de services numériques », le sous-traitant traitera les données à caractère personnel pour le compte du responsable du traitement conformément aux Clauses.

1.4. Les Clauses ont priorité sur toute disposition similaire contenue dans d'autres accords entre les parties.

1.5. Trois annexes sont jointes aux Clauses et en font partie intégrante.

1.6. L'annexe A contient des détails sur le traitement des données à caractère personnel, y compris la finalité et la nature du traitement, le type de données à caractère personnel, les catégories de personnes concernées et la durée du traitement.

1.7. L'annexe B contient les conditions du responsable du traitement pour l'utilisation de sous-traitants ultérieurs par le sous-traitant et la liste des sous-traitants ultérieurs autorisés par le responsable du traitement.

1.8. L'annexe C contient les instructions du responsable du traitement concernant le traitement des données à caractère personnel, les mesures de sécurité minimales à mettre en œuvre par le sous-traitant et la manière dont les audits du sous-traitant et des éventuels sous-traitants ultérieurs doivent être effectués.

1.9. Les Clauses et leurs annexes doivent être conservées par écrit, y compris sous forme électronique, par les deux parties.

1.10. Les Clauses ne dispensent pas le sous-traitant des obligations auxquelles il est soumis en vertu du règlement général sur la protection des données (le RGPD) ou d'autres législations.

2. LES DROITS ET OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

2.1. Le responsable du traitement est chargé de veiller à ce que le traitement des données à caractère personnel soit conforme au RGPD (voir l'article 24 du RGPD), aux dispositions applicables de l'UE ou des États membres en matière de protection des données et aux Clauses.

2.2. Le responsable du traitement a le droit et l'obligation de prendre des décisions sur les finalités et les moyens du traitement des données à caractère personnel.

2.3. Le responsable du traitement est notamment chargé de veiller à ce que le traitement des données à caractère personnel que le sous-traitant est chargé d'effectuer repose sur une base juridique.

3. LE SOUS-TRAITANT AGIT CONFORMÉMENT AUX INSTRUCTIONS

3.1. Le sous-traitant ne doit traiter les données à caractère personnel que sur instruction documentée du responsable du traitement, à moins que le droit de l'Union ou de l'État membre auquel le sous-traitant est soumis ne l'y oblige. Ces instructions sont précisées aux annexes A et C. Des instructions ultérieures peuvent également être données par le responsable du traitement pendant toute la durée du traitement des données à caractère personnel, mais ces instructions doivent toujours être documentées et conservées par écrit, y compris sous forme électronique, en relation avec les Clauses.

3.2. Le sous-traitant doit informer immédiatement le responsable du traitement si les instructions données par le responsable du traitement, de l'avis du sous-traitant, contreviennent au RGPD ou aux dispositions applicables de l'UE ou des États membres en matière de protection des données.

4. CONFIDENTIALITÉ

4.1. Le sous-traitant n'accorde l'accès aux données à caractère personnel traitées pour le compte du responsable du traitement qu'aux personnes placées sous l'autorité du sous-traitant qui se sont engagées à respecter la confidentialité ou qui sont soumises à une obligation légale appropriée de confidentialité, et uniquement sur la base du besoin d'en connaître. La liste des personnes auxquelles l'accès a été accordé fait l'objet d'un réexamen périodique. Sur la base de ce réexamen, l'accès aux données à caractère personnel peut être retiré, si l'accès n'est plus nécessaire, et les données à caractère personnel ne sont dès lors plus accessibles à ces personnes.

4.2. À la demande du responsable du traitement, le sous-traitant doit alors démontrer que les personnes concernées placées sous son autorité sont soumises à la confidentialité susmentionnée

5. SÉCURITÉ DU TRAITEMENT

5.1. L'article 32 du RGPD stipule que, compte tenu de l'état de l'art, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que du risque, dont la probabilité et la gravité varient, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant doivent mettre en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité adapté au risque.

Le responsable du traitement doit évaluer les risques pour les droits et libertés des personnes physiques inhérents au traitement et mettre en œuvre des mesures pour atténuer ces risques. En fonction de leur pertinence, les mesures peuvent comprendre les éléments suivants :

a. Pseudonymisation et chiffrement des données à caractère personnel ;

b. la capacité d'assurer en permanence la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de traitement ;

c. la capacité de rétablir la disponibilité et l'accès aux données à caractère personnel en temps utile en cas d'incident physique ou technique ;

d. un processus permettant de tester, d'apprécier et d'évaluer régulièrement l'efficacité des mesures techniques et organisationnelles destinées à garantir la sécurité du traitement.

5.2. Conformément à l'article 32 du RGPD, le sous-traitant doit également (indépendamment du responsable du traitement) évaluer les risques inhérents au traitement pour les droits et libertés des personnes physiques et mettre en œuvre des mesures pour atténuer ces risques. À cet effet, le responsable du traitement doit fournir au sous-traitant toutes les informations nécessaires à l'identification et à l'évaluation de ces risques.

5.3. En outre, le sous-traitant doit aider le responsable du traitement à s'acquitter des obligations qui lui incombent en vertu de l'article 32 du RGPD, notamment en lui fournissant des informations sur les mesures techniques et organisationnelles déjà mises en œuvre par le sous-traitant en vertu de l'article 32 du RGPD, ainsi que toutes les autres informations nécessaires pour que le responsable du traitement puisse s'acquitter de l'obligation qui lui incombe en vertu de l'article 32 du RGPD.

Si, par la suite, dans l'évaluation du responsable du traitement, l'atténuation des risques identifiés nécessite la mise en œuvre par le sous-traitant de mesures supplémentaires par rapport à celles qu'il a déjà mises en œuvre en vertu de l'article 32 du RGPD, le responsable du traitement doit spécifier ces mesures supplémentaires à mettre en œuvre dans l'annexe C.

6. UTILISATION DE SOUS-TRAITANTS ULTÉRIEURS

6.1. Le sous-traitant doit satisfaire aux exigences énoncées à l'article 28, paragraphes 2 et 4 du RGPD pour faire appel à un autre sous-traitant (un sous-traitant ultérieur).

6.2. Le sous-traitant ne doit donc pas faire appel à un autre sous-traitant (sous-traitant ultérieur) pour l'exécution des Clauses sans l'autorisation écrite générale préalable du responsable du traitement.

6.3. Le sous-traitant dispose de l'autorisation générale du responsable du traitement pour faire appel à des sous-traitants ultérieurs. Le sous-traitant informe par écrit le responsable du traitement de toute modification envisagée concernant l'ajout ou le remplacement de sous-traitants ultérieurs au moins 6 semaines à l'avance, ce qui donne au responsable du traitement la possibilité de s'opposer à ces modifications avant de faire appel au(x) sous-traitant(s) ultérieur(s) concernés. Des délais de préavis plus longs pour des services de sous-traitance ultérieure spécifiques peuvent être prévus à l'annexe B. La liste des sous-traitants ultérieurs secondaires déjà autorisés par le responsable du traitement figure à l'annexe B.

6.4. Lorsque le sous-traitant fait appel à un sous-traitant ultérieur pour effectuer des activités de traitement spécifiques pour le compte du responsable du traitement, les mêmes obligations en matière de protection des données que celles énoncées dans les Clauses sont imposées à ce sous-traitant ultérieur au moyen d'un contrat ou d'un autre acte juridique en vertu du droit de l'UE ou des États membres, en particulier en fournissant des garanties suffisantes pour mettre en œuvre les mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences des Clauses et du RGPD.

Il incombe donc au sous-traitant d'exiger que le sous-traitant ultérieur respecte au moins les obligations auxquelles le sous-traitant est soumis en vertu des Clauses et du RGPD.

6.5. À la demande du responsable du traitement, une copie de cet accord de sous-traitance ultérieure et de ses modifications ultérieures doit être soumise au responsable du traitement, ce qui donne au responsable du traitement la possibilité de s'assurer que ces obligations en matière de protection des données telles qu'énoncées dans les Clauses sont imposées au sous-traitant ultérieur. Les clauses relatives à des questions d'ordre commercial qui n'affectent pas le contenu juridique de l'accord de sous-traitance ultérieure en matière de protection des données ne doivent pas nécessairement être soumises au responsable du traitement.

6.6. Le sous-traitant doit convenir avec le sous-traitant ultérieur d'une clause de tiers bénéficiaire en vertu de laquelle, en cas de faillite du sous-traitant ultérieur, le responsable du traitement est un tiers bénéficiaire de l'accord de sous-traitance ultérieure et a le droit de faire appliquer l'accord au sous-traitant ultérieur auquel fait appel le sous-traitant, ce qui permet par exemple au responsable du traitement d'ordonner au sous-traitant ultérieur de supprimer ou de restituer les données à caractère personnel.

6.7. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant reste pleinement responsable vis-à-vis du responsable du traitement en ce qui concerne l'exécution des obligations du sous-traitant ultérieur. Ceci n'affecte pas les droits des personnes concernées en vertu du RGPD (ceux prévus aux articles 79 et 82 du RGPD) à l'encontre du responsable du traitement et du sous-traitant, y compris le sous-traitant ultérieur.

7. TRANSFERT DE DONNÉES VERS DES PAYS TIERS OU À DES ORGANISATIONS INTERNATIONALES

7.1. Tout transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales par le sous-traitant ne peut avoir lieu que sur instruction documentée du responsable du traitement et doit toujours se faire dans le respect du chapitre V du RGPD.

7.2. Si des transferts vers des pays tiers ou à des organisations internationales, que le sous-traitant n'a pas été chargé d'effectuer par le responsable du traitement, sont requis par le droit de l'UE ou de l'État membre auquel le sous-traitant est soumis, le sous-traitant doit informer le responsable du traitement de cette exigence légale avant le traitement, à moins que le droit en question n'interdise cette information pour des raisons importantes d'intérêt public.

a. Sans instructions documentées de la part du responsable du traitement, le sous-traitant ne peut donc pas, dans le cadre des Clauses :

b. transférer des données à caractère personnel à un responsable du traitement ou à un sous-traitant dans un pays tiers ou dans une organisation internationale ;
c. transférer le traitement des données à caractère personnel à un sous-traitant dans un pays tiers ;
d. faire traiter les données à caractère personnel par le sous-traitant dans un pays tiers.

7.3. Les instructions du responsable du traitement concernant le transfert de données à caractère personnel vers un

pays tiers, y compris, le cas échéant, l'outil de transfert prévu au chapitre V du RGPD sur lequel elles se fondent, doivent figurer à l'annexe C.6.

7.4. Les Clauses ne doivent pas être confondues avec les clauses types de protection des données au sens de l'article 46, paragraphe 2, points c) et d), du RGPD, et les Clauses ne peuvent être invoquées par les parties en tant qu'outil de transfert au titre du chapitre V du RGPD.

8. ASSISTANCE AU RESPONSABLE DU TRAITEMENT

8.1. Compte tenu de la nature du traitement, le sous-traitant doit assister le responsable du traitement par des mesures techniques et organisationnelles appropriées, dans la mesure du possible, dans l'exécution des obligations du responsable du traitement de répondre aux demandes d'exercice des droits de la personne concernée prévues au chapitre III du RGPD.

Cela signifie que le sous-traitant doit, dans la mesure du possible, aider le responsable du traitement à respecter :

a. le droit d'être informé lors de la collecte de données à caractère personnel auprès de la personne concernée ;

b. le droit d'être informé lorsque les données à caractère personnel n'ont pas été obtenues auprès de la personne concernée ;

c. le droit d'accès de la personne concernée ;

d. le droit de rectification ;

e. le droit à l'effacement (« droit à l'oubli ») ;

f. le droit à la limitation du traitement ;

g. l'obligation de notification concernant la rectification ou l'effacement des données à caractère personnel ou la limitation du traitement ;

h. le droit à la portabilité des données ;

i. le droit d'opposition ;

j. le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage.

8.2. Outre l'obligation du sous-traitant d'aider le responsable du traitement en vertu de la Clause 6.3, le sous-traitant doit, compte tenu de la nature du traitement et des informations dont il dispose, aider le responsable du traitement à assurer le respect de :

a. L'obligation pour le responsable du traitement de notifier la violation de données à caractère personnel dans les meilleurs délais et, si possible, au plus tard 72 heures après en avoir pris connaissance ; à l'égard de l'autorité de contrôle compétente dont relève le responsable du traitement, sauf s'il est peu probable que la violation de données à caractère personnel entraîne un risque pour les droits et libertés des personnes physiques ; l'obligation pour le responsable du traitement de communiquer dans les meilleurs délais la violation de données à caractère personnel à la personne concernée, lorsque la violation de données à caractère personnel est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques ;

b. l'obligation pour le responsable du traitement de procéder à une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel (analyse d'impact relative à la protection des données) ;

c. l'obligation pour le responsable du traitement de consulter l'autorité de contrôle compétente dont il relève avant le traitement lorsqu'une analyse d'impact relative à la protection des données indique que le traitement entraînerait un risque élevé en l'absence de mesures prises par le responsable du traitement pour atténuer le risque.

8.3. Les parties doivent définir à l'annexe C les mesures techniques et organisationnelles appropriées par lesquelles le sous-traitant est tenu d'assister le responsable du traitement, ainsi que la portée et l'étendue de l'assistance requise. Ceci s'applique aux obligations prévues aux Clauses 9.1 et 9.2.

9. NOTIFICATION DES VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL

9.1. En cas de violation de données à caractère personnel, le sous-traitant doit notifier cette violation au responsable du traitement dans les meilleurs délais après en avoir pris connaissance.

9.2. La notification du sous-traitant au responsable du traitement doit avoir lieu, si possible, dans les 24 HEURES suivant le moment où le sous-traitant a pris connaissance de la violation de données à caractère personnel pour permettre au responsable du traitement de se conformer à son obligation de notifier la violation de données à caractère personnel à l'autorité de contrôle compétente, conformément à l'article 33 du RGPD.

9.3. Conformément à la clause 9, paragraphe 2, point a), le sous-traitant doit aider le responsable du traitement à notifier la violation de données à caractère personnel à l'autorité de contrôle compétente, ce qui signifie que le sous-traitant est tenu d'aider à obtenir les informations énumérées ci-dessous qui, conformément à l'article 33, paragraphe 3, du RGPD, doivent être mentionnées dans la notification du responsable du traitement à l'autorité de contrôle compétente :

a. La nature des données à caractère personnel, y compris, si possible, les catégories et le nombre approximatif de personnes concernées, ainsi que les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;

b. les conséquences probables de la violation de données à caractère personnel ;

c. les mesures prises ou proposées par le responsable du traitement pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures visant à en atténuer les éventuels effets négatifs.

9.4. Les parties définissent à l'annexe C tous les éléments que le sous-traitant doit fournir lorsqu'il aide le responsable du traitement à notifier une violation de données à caractère personnel à l'autorité de contrôle compétente.

10. EFFACEMENT ET RESTITUTION DES DONNÉES

10.1. À la fin de la prestation de services de traitement de données à caractère personnel, le sous-traitant est tenu de supprimer toutes les données à caractère personnel traitées pour le compte du responsable du traitement et de certifier au responsable du traitement qu'il l'a fait, à moins que le droit de l'Union ou des États membres n'exige la conservation des données à caractère personnel.
Le sous-traitant s'engage à traiter les données à caractère personnel exclusivement pour les finalités et la durée prévues par cette loi et dans les strictes conditions applicables.

11. AUDIT ET INSPECTION

11.1. Le sous-traitant doit mettre à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations énoncées à l'article 28 et dans les Clauses, ainsi que permettre et contribuer aux audits, y compris les inspections, effectués par le responsable du traitement ou par un autre auditeur mandaté par le responsable du traitement.

11.2. Les procédures applicables aux audits, y compris les inspections, du responsable du traitement et des sous-traitants ultérieurs sont spécifiées aux annexes C.7.

11.3. Le sous-traitant est tenu de fournir aux autorités de contrôle qui, en vertu de la législation applicable, ont accès aux installations du responsable du traitement et du sous-traitant, ou aux représentants agissant au nom de ces autorités de contrôle, l'accès aux installations physiques du sous-traitant sur présentation d'une preuve d'identité appropriée.

12. L'ACCORD DES PARTIES SUR D'AUTRES CONDITIONS

12.1. Les parties peuvent convenir d'autres clauses concernant la prestation du service de traitement des données à caractère personnel, notamment en matière de responsabilité, si elles ne contredisent pas directement ou indirectement les Clauses et ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées ni à la protection offerte par le RGPD.

13. ENTRÉE EN VIGUEUR ET RÉSILIATION

13.1. Les Clauses entrent en vigueur à la date de la signature des deux parties.

13.2. Les deux parties ont le droit de demander une renégociation des Clauses si des modifications de la loi ou l'inopportunité des Clauses devaient donner lieu à une telle renégociation.

13.3. Les Clauses s'appliquent pendant toute la durée de la prestation de services de traitement de données à caractère personnel. Pendant la durée de la prestation de services de traitement de données à caractère personnel, les Clauses ne peuvent être résiliées, à moins que d'autres Clauses régissant la prestation de services de traitement de données à caractère personnel n'aient été convenues entre les parties.

13.4. Si la prestation de services de traitement des données à caractère personnel prend fin et que les données à caractère personnel sont supprimées ou restituées au responsable du traitement conformément à la clause 11.1 et à l'annexe C.4, les Clauses peuvent être résiliées par notification écrite de l'une ou l'autre des parties.

14. POINT DE CONTACT DU RESPONSABLE DE LA PROTECTION DES DONNÉES

14.1. Le responsable du traitement peut à tout moment contacter le responsable de la protection des données de Tjekvik au sujet du traitement des données à caractère personnel effectué par le sous-traitant. Le responsable de la protection des données peut être contacté par e-mail : legal@tjekvik.com.

15. SIGNATURE

Pour le compte du responsable du traitement, l'accord sur la protection des données est appliqué conformément aux conditions générales spécifiées.

Pour le compte du sous-traitant

Nom Christian Mark
Poste Directeur général

Signature 

ANNEXE A

INFORMATIONS
sur le traitement

Le traitement des données à caractère personnel par Tjekvik, le sous-traitant, pour le Responsable du traitement, se limite aux données visées à l'article 6.

Les données à caractère personnel concernant les clients du responsable du traitement sont supprimées dans un délai de 15 jours.

Les données à caractère personnel concernant les employés du Responsable du traitement (noms, adresses e-mail et rôles d'utilisateur) sont traitées par Tjekvik pour s'assurer que l'utilisateur individuel a un accès correct au backend de Tjekvik. Les utilisateurs et leurs données peuvent être gérés directement par l'administrateur du compte (de manière centralisée dans plusieurs ateliers) ou par les chefs d'atelier (chef d'atelier local). Les données sont stockées aussi longtemps que le responsable du traitement en a besoin.

A.1.
LA FINALITÉ DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL PAR LE SOUS-TRAITANT POUR LE COMPTE DU RESPONSABLE DU TRAITEMENT EST :

Le produit est une technologie de libre-service intuitive pour l'industrie automobile, qui permet aux clients d'effectuer le check-in et le check-out comme ils le souhaitent, quand ils le souhaitent et où ils le souhaitent : chez eux, en concession grâce à un kiosque intérieur ou en toute sécurité à l'extérieur grâce à un kiosque extérieur.

Le client effectue le check-in et le check-out avec son numéro de téléphone ou sa plaque d'immatriculation.

Les données sont traitées dans le but de :

- Permettre au client de commencer le check-in avant le début du rendez-vous programmé ;
- Permettre au client d'utiliser le libre-service lors du check-in ;
- Permettre au client d'utiliser le libre-service lors du check-out ;

A.2.
LE TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL EFFECTUÉ PAR LE SOUS-TRAITANT POUR LE COMPTE DU RESPONSABLE DU TRAITEMENT PORTE PRINCIPALEMENT SUR (LA NATURE DU TRAITEMENT) :

- La collecte,
- l'enregistrement,
- l'organisation,
- la structuration,
- le stockage,
- la récupération,
- l'utilisation,
- l'alignement ou la combinaison,
- la restriction,
- l'effacement ou la destruction.

A.3.
LE TRAITEMENT PORTE SUR LES TYPES DE DONNÉES À CARACTÈRE PERSONNEL SUIVANTS RELATIFS AUX PERSONNES CONCERNÉES :

- Nom,
- adresse,
- adresse e-mail,

- numéro de téléphone,
- numéro d'enregistrement,
- code VIN,
- détails concernant le véhicule spécifique, c'est-à-dire la marque, le modèle,
- détails de la commande, c'est-à-dire le contenu du travail prévu et, dans certains cas, le prix.

A.4.
LE TRAITEMENT COMPREND LES CATÉGORIES SUIVANTES DE PERSONNES CONCERNÉES :

- Clients actuels de l'atelier du responsable du traitement.
- Employés du responsable du traitement.

A.5.
LE TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL PAR LE SOUS-TRAITANT POUR LE COMPTE DU RESPONSABLE DU TRAITEMENT PEUT ÊTRE EFFECTUÉ LORSQUE LES CLAUSES ENTRENT EN VIGUEUR. LE TRAITEMENT A LA DURÉE SUIVANTE :

La durée de chaque traitement pour la personne concernée est généralement de 9 jours, à partir du moment où le sous-traitant importe les données depuis une API. Au bout de 9 jours, le système efface les données à caractère personnel.

Dans certains cas, nous traitons les données pendant un maximum de 15 jours. Cela se produit lorsque le sous-traitant importe les données depuis un système CSV et non depuis une solution API.

ANNEXE B

Sous-traitants ultérieurs
AUTORISÉS

B.1.
SOUS-TRAITANTS ULTÉRIEURS AGRÉÉS
Dès l'entrée en vigueur des clauses, le responsable du traitement autorise à faire appel aux sous-traitants ultérieurs suivants :

NOM	CVR	ADRESSE	DESCRIPTION DU TRAITEMENT	BASES LÉGALES
HEROKU	**Numéro d'identification fiscale américain :** 26-1088476 **Numéro d'entreprise :** C3096268	Heroku fait partie de Salesforce, et son siège social est situé à : 415 Mission Street Suite 300 San Francisco, CA 94105	Hébergement cloud de l'application Tjekvik (sur des serveurs AWS) AWS DUB2 est situé au 4033 Citywest Avenue, Cooldown Commons, County Dublin, Irlande et le centre de redondance Amazon AWS FRA54 est situé au Eschborner Landstraße 100, 60489 Frankfurt am Main, Allemagne. Les données à caractère personnel de vos clients ne quittent pas l'UE.	Salesforce, y compris Heroku, qui est un sous-traitant ultérieur basé aux États-Unis a certifié au Département du Commerce des États-Unis qu'il se conforme aux principes du cadre de protection des données UE-États-Unis (Principes DPF UE - États-Unis) concernant le traitement des données à caractère personnel reçues de l'Union européenne et du Royaume-Uni dans le cadre de l'accord entre l'UE et les États-Unis.
AMAZON	**Numéro d'entreprise :** C3568304	Siège social : 410 Terry Avenue North, Seattle, WA 98109-5210	Hébergement cloud du serveur SFTP utilisé pour les importations de rendez-vous via des fichiers CSV La région Europe est située dans le principal centre de données européen d'Amazon Web Services en Irlande. 4033 Citywest Avenue, Cooldown Commons, County Dublin, Irlande et le centre de redondance Amazon AWS FRA54 est situé à Eschborner Landstraße 100, 60489 Frankfurt am Main, Allemagne. Les données à caractère personnel de vos clients ne quittent pas l'UE.	Amazon a certifié au Département du Commerce des États-Unis qu'il se conforme aux principes du cadre de protection des données UE-États-Unis (Principes DPF UE - États-Unis) concernant le traitement des données à caractère personnel reçues de l'Union européenne et du Royaume-Uni dans le cadre de l'accord UE - États-Unis.
TWILIO	**Numéro d'entreprise :** 10994798-0143	Siège social : 375 Beale Street Suite 300 San	Opérations SMS	Twilio a certifié au Département du Commerce des États-Unis qu'il se conforme aux

		Francisco, CA 94105 USA	Le serveur est situé aux États-Unis. La région par défaut de Twilio se trouve dans l'est des États-Unis (É-U), région US1.	principes du cadre de protection des données UE - États-Unis (Principes DPF UE - États-Unis) concernant le traitement des données à caractère personnel reçues de l'Union européenne et du Royaume-Uni dans le cadre de l'accord entre l'UE et les États-Unis.
Ou (vous, en tant que client, choisissez le fournisseur)				
SINCH SWEDEN AB	556747-5495	Lindhagensgatan 74 112 18 Stockholm Suède	Le serveur est situé dans l'UE/EEE à Dublin, en Irlande, et à Francfort, en Allemagne.	
Mailgun	**Numéro d'entreprise :** 0802653513	112 E Pecan St. #1135 San Antonio, TX 78205, États-Unis	Opérations e-mail Allemagne et Belgique. Les données à caractère personnel de vos clients ne quittent pas l'UE.	Clauses contractuelles types (CCT) avec Mailgun du 14 janvier 2022.

Dès l'entrée en vigueur des Clauses, le responsable du traitement autorise le recours aux sous-traitants ultérieurs susmentionnés pour le traitement décrit pour cette partie.

En l'absence d'une décision au titre de l'article 45, paragraphe 3, un responsable du traitement ou un sous-traitant ne peut transférer des données à caractère personnel à un pays tiers ou à une organisation internationale que si le responsable du traitement ou le sous-traitant a fourni des garanties appropriées et à condition que des droits opposables et des voies de recours effectives soient disponibles pour les personnes concernées (cf. article 46, paragraphe 1, du règlement). Des garanties appropriées ont été mises en œuvre avec les sous-traitants ultérieurs susmentionnés, afin de garantir les droits de la personne concernée.

Le 4 juin 2021, la Commission a publié des clauses contractuelles types (CCT) modernisées en vertu du RGPD pour les transferts de données des responsables de traitement ou des sous-traitants dans l'UE/EEE (ou autrement soumis au RGPD) vers les responsables de traitement ou les sous-traitants établis en dehors de l'UE/EEE (et non soumis au RGPD). Voir la DÉCISION D'EXÉCUTION (UE) 2021/914 de la COMMISSION.

Toutes les données à caractère personnel traitées pour le compte du responsable du traitement sont traitées sur le territoire de l'UE/EEE.

B.2.
AVIS PRÉALABLE POUR L'AUTORISATION DES SOUS-TRAITANTS ULTÉRIEURS

Si Tjekvik ajoute un sous-traitant ultérieur pour effectuer des tâches pour lesquelles Tjekvik est le sous-traitant pour le compte du responsable du traitement spécifié dans le présent contrat, une notification préalable sera adressée au responsable du traitement des données au plus tard 6 semaines avant que le changement de sous-traitant ultérieur n'ait lieu.

Si le responsable du traitement s'oppose au changement, il doit le faire dans les meilleurs délais et au plus tard dans les 21 jours suivant la réception de la notification par le responsable du traitement.

ANNEXE C

INSTRUCTION RELATIVE
à l'utilisation des données à caractère personnel

C.1.
L'OBJET/INSTRUCTION DU TRAITEMENT

Le traitement des données à caractère personnel par le sous-traitant pour le compte du responsable du traitement est effectué par le sous-traitant selon les modalités suivantes :

Le sous-traitant traite les données à caractère personnel afin de fournir « Tjekvik, réception de service numérique » au responsable du traitement conformément aux Conditions de service.

Les données collectées par Tjekvik proviennent du système DMS ou de l'API du Responsable du traitement. Dans de rares cas, les données sont collectées auprès de la personne concernée, ce qui garantit le droit de rectification et l'exactitude des données traitées.

Les données à caractère personnel feront l'objet de plusieurs activités de traitement, y compris mais sans s'y limiter :

C.2.
SÉCURITÉ DU TRAITEMENT

Le niveau de sécurité tient compte des éléments suivants :

Le traitement porte sur un nombre significatif de données à caractère personnel, qui relèvent de l'article 6 du règlement. Aucune donnée relevant de l'article 9 ou 10 n'est traitée. Le risque de violation des droits et libertés de la personne concernée est faible, ce que reflète le niveau de sécurité.

Le sous-traitant a désormais le droit et l'obligation de prendre des décisions concernant les mesures de sécurité techniques et organisationnelles à appliquer pour créer le niveau nécessaire (et convenu) de sécurité des données.

Toutefois, le sous-traitant doit, en tout état de cause et au minimum, mettre en œuvre les mesures suivantes qui ont été convenues avec le responsable du traitement :

C.2.1. La protection des données est assurée par le directeur de la technologie et le responsable juridique, comme indiqué dans le présent document.

Tjekvik forme ses employés à la protection des données à caractère personnel au sein de l'organisation.

C.2.2. Exigences en matière de chiffrement des données à caractère personnel :

Par défaut, Tjekvik utilise HTTPS entre une API et les comptes utilisateurs. Les mots de passe des utilisateurs sont également chiffrés dans la base de données.

Le contenu transmis sur le réseau est toujours transmis par HTTPS, à l'aide d'un certificat de clé publique 2048 bits. SSLv3 et les versions inférieures, ainsi que TLS 1.0, sont désactivés compte tenu des vulnérabilités publiées dans ces versions et de leurs implications en termes de sécurité.

Lorsque les données sont transférées entre les systèmes, elles sont chiffrées en transit (SFTP/HTTPS). Les concessionnaires ont la possibilité d'acheter un chiffrement supplémentaire (données chiffrées au repos à l'intérieur de la base de données).

C.2.3. Exigences visant à garantir en permanence la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et des services de traitement :

- La collecte,
- l'enregistrement,
- l'organisation,
- la structuration,
- le stockage,
- la récupération,
- l'utilisation,

- l'alignement ou la combinaison,
- la restriction,
- l'effacement ou la destruction.

Tjekvik a permis aux personnes concernées de rectifier des informations, telles que les coordonnées.

Tjekvik a permis aux administrateurs de boutiques et de comptes d'ajouter, de rectifier ou de supprimer des informations.

Une sauvegarde complète des données est effectuée toutes les 6 heures, avec une sauvegarde delta dans l'intervalle.

C.2.4. Exigences relatives à la capacité de rétablir la disponibilité et l'accès aux données à caractère personnel en temps utile en cas d'incident physique ou technique :

Tjekvik ne stocke qu'une quantité très limitée de données pour une période très limitée. Si nécessaire, en raison d'un événement physique ou technique, les données perdues peuvent être réimportées et remises à disposition.

C.2.5. Exigences relatives aux processus permettant de tester, d'apprécier et d'évaluer régulièrement l'efficacité des mesures techniques et organisationnelles destinées à garantir la sécurité du traitement :

Un test d'intrusion est effectué de manière récurrente pour s'assurer que toutes les données à caractère personnel sont stockées en toute sécurité dans le système.

Tous les employés sont informés des lignes directrices relatives au traitement des données à caractère personnel.

C.2.6.

La gestion de l'accès

Contrôle d'accès physique
Tjekvik est une entreprise « full remote » (100 % à distance). Aucune infrastructure n'est hébergée dans un bureau ou un local. La plateforme Tjekvik est basée sur le cloud et toutes les politiques PAC sont gérées par Heroku et AWS et traitées selon les normes officielles.

Contrôle de l'accès au système
L'accès aux ressources numériques est limité aux personnes qui en ont besoin : l'assistance de 1er et 2e niveau principalement, et l'équipe DevOps.
La sécurité est assurée par l'utilisation de clés SSH et la connexion des utilisateurs avec une politique de mot de passe fort et/ou AMF (authentification multi-facteur).

Contrôle de l'accès aux données
L'accès aux ressources de données est limité aux personnes qui en ont besoin : l'assistance de 2e niveau en mode lecture uniquement en production.
La sécurité est assurée par l'utilisation de clés SSH et la connexion des utilisateurs avec une politique de mot de passe fort et/ou AMF (authentification multi-facteur).

Contrôle de la transmission des données
Le contenu transmis sur le réseau est toujours transmis par HTTPS, à l'aide d'un certificat de clé publique 2048 bits. SSLv3 et les versions inférieures, ainsi que TLS 1.0, sont désactivés à la lumière des vulnérabilités publiées dans ces versions et de leurs implications en termes de sécurité.

Contrôle d'entrée
- Les données importées (pour les rendez-vous) à partir de systèmes externes sont vérifiées en termes de cohérence et d'attaques par injection SQL
- Les contrôles d'entrée sont sécurisés par l'utilisation de bibliothèques spécifiques reconnues qui sont utilisées pour chaque version de la plate-forme avant le déploiement pour tester et détecter les vulnérabilités des contrôles d'entrée.
- Un test d'intrusion (effectué par la société Sapphire) a été réalisé en mai 2022. Aucun problème CRITIQUE n'a été détecté, tous les problèmes ÉLEVÉS détectés ont été résolus au cours du troisième trimestre de l'année 2022 et lancés en production. Des tests d'intrusion seront organisés tous les deux ans.

Contrôle de la disponibilité
Un système d'alerte est en place en cas de panne de la plate-forme (tous les composants sont surveillés et déclenchent des alertes séparément)
Le basculement et les redondances seront mis en œuvre en 2024 une fois que l'infrastructure aura été entièrement transférée sur AWS (actuellement, une partie est sur Heroku et une autre sur AWS).

C.3.
ASSISTANCE AU RESPONSABLE DU TRAITEMENT

Le sous-traitant doit assister, dans la mesure du possible (dans le cadre et l'étendue de l'assistance précisée ci-dessous) le responsable du traitement conformément aux clauses 9.1. et 9.2. en mettant en œuvre les mesures techniques et organisationnelles suivantes :

Tjekvik notifiera le responsable du traitement, si possible, dans les 24 HEURES après que Tjekvik a pris connaissance de la violation de données à caractère personnel afin de permettre au responsable du traitement de se conformer à l'obligation du responsable du traitement de notifier la violation de données à caractère personnel à l'autorité de contrôle compétente, conformément à l'article 33 du RGPD.

C.4.
PÉRIODE DE CONSERVATION/PROCÉDURES D'EFFACEMENT

La période de conservation générale est de 14 jours. Si une personne concernée n'a pas récupéré la clé de son véhicule, ses données ne sont pas effacées tant que la clé n'a pas été récupérée.

Cette période peut être prolongée si la source d'importation des rendez-vous provient d'un fichier CSV, car nous conservons alors les rendez-vous utilisés pour le check-in pendant 25 jours, afin de garantir la disponibilité pour le check-out.

C.5.
LIEU DE TRAITEMENT

Le traitement des données à caractère personnel en vertu des Clauses sera effectué dans les lieux indiqués au point B.1 et au bureau de Tjekvik.

C.6.
INSTRUCTION SUR LE TRANSFERT DE DONNÉES À CARACTÈRE PERSONNEL VERS DES PAYS TIERS

Lors du transfert de données vers un pays tiers, qui présente un niveau de protection adéquat (un pays tiers sûr) ou vers un pays tiers sans niveau de sécurité conformément au règlement général sur la protection des données, tous les transferts ont une base légale de transfert.

En ce qui concerne les transferts de données à caractère personnel vers des pays tiers qui ne figurent pas sur la liste des pays tiers sûrs, Tjekvik vérifiera de manière continue, et au moins une fois par an, si le sous-traitant satisfait toujours aux exigences de sécurité relatives au transfert de données à caractère personnel vers des pays tiers, énoncées dans le règlement général sur la protection des données. S'il s'avère que les exigences du règlement ne sont pas respectées, Tjekvik mettra immédiatement fin à la coopération avec le sous-traitant ultérieur et informera le responsable du traitement de la décision de mettre fin à la coopération. En cas de changement de sous-traitant ultérieur, Tjekvik utilisera la procédure convenue décrite au point B.2

C.7.
PROCÉDURES POUR LES AUDITS DU RESPONSABLE DU TRAITEMENT, Y COMPRIS LES INSPECTIONS, DU TRAITEMENT DES DONNÉES EFFECTUÉ PAR LE SOUS-TRAITANT

Le responsable du traitement ou son représentant a le droit d'effectuer une inspection physique annuelle des lieux où le traitement des données à caractère personnel est effectué par le sous-traitant, y compris les installations physiques ainsi que les systèmes utilisés pour le traitement et liés à celui-ci, afin de s'assurer que le sous-traitant respecte le RGPD, les dispositions applicables de l'UE ou des États membres en matière de protection des données et les clauses.

En plus de l'inspection prévue, le responsable du traitement peut effectuer une inspection du sous-traitant lorsque le responsable du traitement le juge nécessaire.