Contrat de sous-traitance conformément à l'art. 28 du RGPD

EASYRENT

conclu entre

ci-après dénommé le «**Donneur d'ordre**», d'une part

et

Wintersteiger Schweiz AG
CHE-109.473.380
Industriestrasse 86
CH – 7310 Bad Radgaz

ci-après dénommé le «**Mandataire**», d'autre part

(également dénommé individuellement la «Partie» et collectivement les «Parties»)

Remarques préliminaires

Le présent contrat de sous-traitance constitue un complément au contrat principal entre les Parties au contrat et précise leurs obligations en matière de protection des données.

Le Mandataire traite les données à caractère personnel pour le compte du Donneur d'ordre au sens de l'art. 4, point 2 et de l'art. 28 du règlement (UE) 2016/679 (règlement général relatif à la protection des données personnelles, RGPD).

Dans le cadre du présent contrat, le Donneur d'ordre est responsable du respect des dispositions légales des lois sur la protection des données, en particulier de la licéité de la transmission des données au Mandataire ainsi que de la licéité du traitement des données («Responsable du traitement» au sens de l'art. 4, point 7 du RGPD).

1. Objet et durée du contrat

1.1 Objet du contrat

L'objet du contrat découle de l'accord/du mandatement existant et des conditions de licence et de maintenance EASYRENT y afférentes, auxquelles nous vous renvoyons ici (ci-après dénommées collectivement: Contrat principal).

1.2 Durée du contrat

La durée du présent contrat (durée) correspond à la durée du contrat principal.

Les dispositions de résiliation du contrat principal sont applicables.

2. Clarification du contenu du contrat

2.1 Nature et finalité du traitement des données à caractère personnel prévu

Le traitement des données est effectué exclusivement aux fins indiquées à l'**Annexe 1**.

2.2 Lieu du traitement des données

2.2.1 La fourniture du traitement des données convenu par contrat a lieu exclusivement dans un État membre de l'Union européenne (UE) ou dans un autre État signataire de l'accord sur l'Espace économique européen (EEE).

2.2.2 Toute délocalisation dans un pays tiers requiert l'approbation préalable du Donneur d'ordre et peut uniquement avoir lieu si les conditions particulières de l'art. 44 et suivants du RGPD sont satisfaites.

2.3 Type de données à caractère personnel

2.3.1 Le type de données à caractère personnel traitées par le Mandataire est défini à l'**Annexe 2**.

2.4 Catégories de personnes concernées

2.4.1 Les personnes concernées par le traitement des données effectué par le Mandataire sont définies à l'**Annexe 3**.

3. Mesures techniques et organisationnelles

3.1 Avant le début du traitement, le Mandataire documentera la mise en œuvre des mesures techniques et organisationnelles discutées avec le Donneur d'ordre avant l'attribution du contrat. La responsabilité de sélectionner les mesures techniques et organisationnelles

appropriées et efficaces incombe au Donneur d'ordre. Dans la mesure où le contrôle par l'autorité compétente en matière de protection des données révèle un besoin d'adaptation, ce dernier est mise en œuvre d'un commun accord dans un délai raisonnable.

3.2 Le Mandataire établira la sécurité par des mesures appropriées conf. à l'art. 28, paragr. 3, lettre c et à l'art. 32 du RGPD notamment en lien avec l'art. 5, paragr. 1 et 2 du RGPD. De manière globale, les mesures à prendre sont des mesures de sécurité des données et visent à assurer un niveau de protection adapté au risque en termes de confidentialité, d'intégrité, de disponibilité et de résilience des systèmes. Dans ce cadre, le Mandataire tiendra compte de l'état de la technique, des frais de mise en œuvre et de la nature, de l'étendue et des finalités du traitement, ainsi que des différences de probabilité et de gravité du risque pour les droits et libertés des personnes physiques au sens de l'art. 32, paragr. 1 du RGPD (détails à l'**Annexe 4**).

3.3 Les mesures techniques et organisationnelles sont soumises au progrès technique et au développement. En ce sens, le Mandataire est autorisé à mettre en œuvre des mesures appropriées alternatives. Le niveau de sécurité des mesures définies ne doit pas être revu à la baisse dans ce cadre. Les modifications importantes doivent être documentées.

4. Pouvoir d'instruction du Donneur d'ordre

4.1 Le Mandataire traitera toutes les données à caractère personnel exclusivement dans le cadre de l'accord passé et en respectant les instructions du Donneur d'ordre (art. 29 du RGPD), dans la mesure où il n'est pas tenu au traitement par le droit de l'Union européenne ou des États membres; dans un tel cas, le Mandataire communiquera au Donneur d'ordre ces exigences légales avant de procéder au traitement, dans la mesure où le droit concerné n'interdit pas une telle communication. Les instructions sont définies d'emblée par le présent contrat et peuvent ensuite être modifiées, complétées ou remplacées par le Donneur d'ordre à travers des instructions individuelles sous forme écrite ou électronique (forme textuelle) adressées à l'organisme indiqué par le Mandataire. Le Mandataire documente les instructions communiquées dans un répertoire tenu par ses soins.

4.2 Le Donneur d'ordre confirmera les instructions orales par écrit ou par voie électronique.

4.3 Le Mandataire devra informer immédiatement le Donneur d'ordre s'il pense que des instructions contreviennent à des dispositions en matière de protection des données. Le Mandataire est autorisé à reporter l'exécution des instructions correspondantes jusqu'à ce que le Donneur d'ordre les ait confirmées ou modifiées par écrit.

4.4 Le Mandataire n'utilisera pas les données à caractère personnel à d'autres fins que celles convenues, notamment en aucun cas à des fins propres ou aux fins de tiers.

4.5 Aucune copie ni aucun double des données ne sera réalisé sans que le Donneur d'ordre en ait connaissance. Font exception à cette disposition les copies de sauvegarde, dans la mesure où elles sont nécessaires afin de garantir un traitement des données en bonne et due forme, ainsi que les données à caractère personnel nécessaires dans le but de respecter les obligations de conservation légales.

5. Correction, limitation et effacement des données à caractère personnel

5.1 Dans la mesure où une personne concernée soumet directement au Mandataire une requête concernant ses données à caractère personnel traitées en sous-traitance

conformément à ses droits légaux d'accès, de rectification, d'effacement, de limitation du traitement, de portabilité des données, d'opposition et de refus d'une prise de décision fondée exclusivement sur une décision automatisée (art. 15 à 22 du RGPD, collectivement: Droits des personnes concernées), le Mandataire transmettra immédiatement cette requête au Donneur d'ordre. Le Mandataire ne sera pas responsable de l'absence de réponse, du retard de la réponse ou d'une réponse défectueuse à la requête de la personne concernée transmise au Donneur d'ordre.

5.2 Le Mandataire ne corrigera pas, n'effacera pas ou ne limitera pas le traitement des données à caractère personnel de la personne concernée soumettant la requête de sa propre initiative, mais uniquement conformément aux instructions documentées du Donneur d'ordre. Il en va de même pour l'exécution du droit d'accès et du droit à la portabilité des données de la personne concernée.

5.3 Sans préjudice de la disposition du paragraphe 1, le Mandataire est autorisé à effacer des données à caractère personnel après en avoir préalablement informé le Donneur d'ordre, si et dans la mesure où cela est nécessaire au bon fonctionnement de la prestation définie dans le Contrat principal et où la possibilité est donnée au Donneur d'ordre d'exporter une sauvegarde de données.

5.4 Le Mandataire devra être dédommagé pour les coûts qu'il a encourus afin d'aider le Donneur d'ordre à défendre les droits de la personne concernée en vertu du présent point 5.

6. Coordonnées du délégué à la protection des données ou de l'interlocuteur pour la protection des données

6.1 Le Mandataire nommera par écrit un délégué à la protection des données qui exercera son activité conformément aux art. 38 et 39 du RGPD si le Mandataire y est tenu par la loi.

6.2 Le Mandataire n'est pas tenu de nommer un délégué à la protection des données. Est nommé en tant qu'interlocuteur chez le Mandataire:

Nom: Sandro Gruber
Tél.: +41 41 783 83 71
E-mail: datenschutz@wintersteiger.ch

6.3 Les éventuelles modifications des coordonnées doivent être immédiatement communiquées au Donneur d'ordre.

7. Préservation de la confidentialité

7.1 Dans l'exécution de ses tâches, le Mandataire fera uniquement intervenir des employés tenus à la confidentialité et ayant été préalablement familiarisés avec les dispositions applicables dans leur cas en matière de protection des données. Le Mandataire et toute personne subordonnée au Mandataire ayant accès aux données à caractère personnel sont uniquement autorisés à traiter ces données conformément aux instructions du Donneur d'ordre dans le cadre des pouvoirs accordés dans le présent contrat, à moins qu'ils ne soient tenus par la loi au traitement de ces données.

7.2 L'obligation de confidentialité persiste après la fin du contrat.

8. Obligation de contrôle et de justification du Mandataire

8.1 Le Mandataire contrôle régulièrement les processus internes ainsi que les mesures techniques et organisationnelles conformément à l'**Annexe 4**, afin de garantir que le traitement effectué dans son domaine de responsabilité est réalisé dans le respect des exigences applicables en matière de protection des données et de veiller à ce que la protection des droits des personnes concernées soit garantie.

8.2 Sur demande, le Mandataire justifiera auprès du Donneur d'ordre des mesures techniques et organisationnelles prises dans le cadre de ses pouvoirs de contrôle conformément au point 10. du présent contrat.

9. Relations de sous-traitance

9.1 Il y a relation de sous-traitance lorsque le Mandataire mandate d'autres sous-traitants (Sous-traitants ultérieurs) pour la fourniture de tout ou partie des prestations dues au Donneur d'ordre sur la base du contrat. Le Mandataire sélectionnera minutieusement les Sous-traitants ultérieurs en tenant tout particulièrement compte des mesures techniques et organisationnelles prises par ces derniers et passera avec eux des accords dans la mesure nécessaire, afin de garantir des mesures de protection des données et de sécurité des informations appropriées.

9.2 Les relations de sous-traitance au sens de la présente disposition ne comprennent pas les prestations de services que le Mandataire utilise en tant que prestations annexes pour aider à la sous-traitance. Ces prestations annexes comprennent par ex. les prestations de télécommunication, les prestations postales et de transport, la maintenance et le service aux utilisateurs (dans la mesure où le prestataire n'a pas accès aux données à caractère personnel), les services de nettoyage ou l'élimination de supports de données. Afin de garantir également la protection et la sécurité des données à caractère personnel du Donneur d'ordre dans les prestations annexes de ce type, le Mandataire est toutefois tenu de passer des accords contractuels appropriés et conformes à la législation ainsi que de prendre des mesures de contrôle.

9.3 Le Mandataire est autorisé à faire appel à des Sous-traitants ultérieurs.

9.4 Le Donneur d'ordre consent à ce que le Mandataire mandate les Sous-traitants ultérieurs énumérés à l'**Annexe 5**.

9.5 Le Mandataire devra informer le Donneur d'ordre avant d'ajouter de nouveaux Sous-traitants ultérieurs ou de changer un Sous-traitant ultérieur figurant dans la liste. Le Donneur d'ordre peut s'opposer à la modification pour un motif important dans les 14 jours faisant suite à la communication de la modification. Si le Donneur d'ordre ne s'y oppose pas dans ce délai, la modification sera réputée approuvée. Si le Donneur d'ordre s'oppose au mandatement du Sous-traitant ultérieur et si le Mandataire est dans l'incapacité de mandater rapidement un autre Sous-traitant ultérieur à des conditions appropriées, le Mandataire pourra soit ajuster la rémunération convenue aux coûts plus élevés engendrés par l'autre Sous-traitant ultérieur, soit résilier le présent contrat et le contrat principal de façon extraordinaire.

9.6 Si le Mandataire confie des missions à des Sous-traitants ultérieurs, il transfère ainsi ses obligations relevant du droit en matière de protection des données issues du contrat au Sous-traitant ultérieur conformément à l'art. 28, paragr. 4 et 9 du RGPD dans la mesure où cela est applicable et raisonnable. À cette fin, il passera un accord écrit avec les Sous-traitants ultérieurs. Le Mandataire devra contrôler régulièrement le respect de ces obligations.

10. Droits de contrôle du Donneur d'ordre

10.1 D'un commun accord avec le Mandataire, le Donneur d'ordre est en droit, une fois par an, d'effectuer ou de faire effectuer des contrôles par un contrôleur à nommer à chaque fois et de s'assurer par des contrôles ponctuels que le Mandataire respecte le présent accord dans le cadre de ses activités commerciales. Le Donneur d'ordre fera uniquement exécuter ces contrôles par du personnel suffisamment qualifié et tenu à la confidentialité, ou par des contrôleurs externes suffisamment qualifiés et tenus à la confidentialité à désigner au cas par cas, après en avoir notifié en temps utile le Mandataire, le contrôle devant être effectué pendant les heures normales d'ouverture et sans perturber le déroulement des opérations. Le Donneur d'ordre remettra au Mandataire une copie du rapport de contrôle.

10.2 Le Mandataire veillera à ce que le Donneur d'ordre puisse être convaincu du respect des obligations du Mandataire conformément à l'art. 28 du RGPD. Sur demande, le Mandataire fournira au Donneur d'ordre les informations nécessaires et justifiera en particulier de la mise en œuvre des mesures techniques et organisationnelles.

10.3 La preuve de telles mesures, qui ne se rapportent pas uniquement à la mission spécifique, peut notamment être apportée par le respect de codes de conduite approuvés conformément à l'art. 40 du RGPD; par une certification selon une procédure de certification approuvée conformément à l'art. 42 du RGPD; par des attestations, rapports ou extraits de rapports actuels d'instances indépendantes (par ex. de commissaires aux comptes, d'auditeurs, du délégué à la protection des données, du service sécurité informatique, d'auditeurs de la protection des données, d'auditeurs qualité); par une certification adaptée dans le cadre d'un audit de la sécurité informatique ou de la protection des données (par ex. d'après l'office fédéral de la sécurité des technologies de l'information).

10.4 Le Mandataire devra être dédommagé de façon raisonnable pour avoir permis au Donneur d'ordre de réaliser des contrôles et pour avoir collaboré aux contrôles.

11. Communication et comportement du Mandataire en cas de manquements

11.1 Sur demande écrite, le Mandataire sera tenu d'assister le Donneur d'ordre et de collaborer avec ce dernier en ce qui concerne le respect des obligations mentionnées aux articles 32 à 36 du RGPD portant sur la sécurité des données à caractère personnel, les obligations de signalement en cas de pannes de données, les analyses d'impact relatives à la protection des données et les consultations préalables, dans la mesure nécessaire et raisonnable. En font notamment partie

a) le fait de veiller à un niveau de protection adapté par des mesures techniques et organisationnelles tenant compte des circonstances et des finalités du traitement ainsi que de la probabilité et de la difficulté prévues d'une potentielle violation des droits par des failles de sécurité et le fait de déclarer immédiatement les événements pertinents liés à une violation;

b) l'obligation de signaler immédiatement les violations de données à caractère personnel au Donneur d'ordre;

c) l'obligation d'assister le Donneur d'ordre dans le cadre de son obligation d'information vis-à-vis des personnes concernées et de mettre immédiatement à sa disposition l'ensemble des informations pertinentes dans ce cadre;

d) le fait d'assister le Donneur d'ordre dans son analyse d'impact relative à la protection des données;

e) le fait d'assister le Donneur d'ordre dans le cadre de ses consultations préalables avec les autorités de contrôle.

11.2 Le Mandataire peut demander une rémunération raisonnable pour les prestations d'assistance mentionnées.

11.3 Les dispositions ci-dessus continuent de s'appliquer sans modification après la fin du présent contrat jusqu'à l'exécution complète des obligations qui y sont mentionnées.

12. Effacement et restitution des données à caractère personnel

12.1 Au cours des 6 mois faisant suite à la fin de la durée du présent accord ou avant sur demande du Donneur d'ordre, le Mandataire remettra au Donneur d'ordre l'ensemble des documents en sa possession, des résultats du traitement et de l'utilisation créés, ainsi que l'ensemble des données en lien avec la relation de sous-traitance, ou effacera ou détruira ces données après accord préalable d'une manière conforme à la protection des données, dans la mesure où aucun intérêt légitime du Mandataire ne s'y oppose. La disposition ci-dessus ne s'applique pas lorsque l'effacement n'est pas possible ou lorsque cet effacement demanderait un effort impossible ou disproportionné pour le Mandataire.

12.2 Les documentations servant à justifier d'un traitement des données conforme à la mission et en bonne et due forme, ou servant à la défense de droits, pourront être conservées par le Mandataire par-delà la fin du contrat conformément aux délais de conservation légaux ou contractuels applicables. Pour être libéré de ses obligations, il peut les remettre au Donneur d'ordre à la fin du contrat.

13. Autres obligations du Mandataire

13.1 Sur demande écrite, le Mandataire sera tenu d'assister le Donneur d'ordre et de collaborer avec ce dernier dans le cadre de l'exécution des droits des personnes concernées conformément aux art. 12 à 22 du RGPD dans la mesure nécessaire et raisonnable. Il devra communiquer au Donneur d'ordre les informations nécessaires de la façon appropriée.

13.2 Le Mandataire peut demander une rémunération raisonnable pour les prestations d'assistance mentionnées.

14. Dispositions finales

14.1 Si la propriété du Donneur d'ordre chez le Mandataire est menacée par des mesures de tiers (par ex. par une saisie ou une confiscation), par une procédure d'insolvabilité ou par d'autres événements, le Mandataire en informera immédiatement le Donneur d'ordre. Le Mandataire informera immédiatement toutes les personnes responsables dans ce cadre du fait que des données à caractère personnel sont traitées dans le cadre de la mission et du fait que la souveraineté sur ces données revient au Donneur d'ordre.

14.2 Les modifications et les compléments apportés au présent accord requièrent la forme écrite, dans la mesure où la loi n'impose pas une forme plus stricte. Ceci s'applique également à une dérogation de la présente clause de forme écrite.

14.3 Si l'une des dispositions du présent accord s'avérait ou devenait partiellement ou totalement invalide ou inexécutable, la validité des autres dispositions ne s'en trouverait pas affectée.

14.4 Le droit autrichien est seul applicable au présent accord, y compris en ce qui concerne son établissement. La Convention des Nations Unies sur les contrats de vente internationale de marchandises n'est pas applicable. La juridiction exclusivement compétente pour tous les litiges issus de ou en lien avec le présent accord, y compris les litiges sur son établissement, est le tribunal de Ried im Innkreis ayant la compétence matérielle.

Hünenberg, le , le

_____ _____

Wintersteiger Schweiz AG
Daniel Kisslig, président du Conseil d'administration
Daniel Steininger, délégué du Conseil d'administration

Annexe 1

Nature et finalités du traitement des données

Le Mandataire traite les données à caractère personnel mises à disposition par le Donneur d'ordre ou collectées ou traitées d'une autre manière pour le compte du Mandataire dans le cadre de la fourniture des services aux fins suivantes:

X Télémaintenance et assistance Easyrent

□ Réservation en ligne / Enregistrement (hébergement) Easyrent

- □ Envoi d'e-mails via Sendgrid

Annexe 2

Données à caractère personnel concernées par le traitement des données

Le Mandataire traite les catégories de données à caractère personnel suivantes mises à disposition par le Donneur d'ordre, ou collectées ou traitées d'une autre manière pour le compte du Mandataire dans le cadre de la fourniture des services:

- données de base des personnes
- données de communication (par ex. téléphone, e-mail)
- historique du client/de la cliente
- données de facturation et de paiement
- données de base des employées
- données d'identité

Parmi les données à caractère personnel, les catégories spéciales de données à caractère personnel suivantes sont représentées:

- aucune
- origine raciale et ethnique
- opinion politique
- conviction religieuse ou idéologique
- données génétiques ou biométriques
- données de santé
- données sur la vie ou l'orientation sexuelle
- données sur les condamnations pénales et les infractions

Annexe 3

Personnes concernées par le traitement des données

Le Mandataire traite les données à caractère personnel mises à disposition par le Donneur d'ordre, ou collectées ou traitées d'une autre manière pour le compte du Mandataire dans le cadre de la fourniture des services pour les catégories de personnes concernées suivantes:

employés

consommateurs, clients finaux

fournisseurs

enfants (jusqu'à l'âge de 14 ans)

Annexe 4

Mesures techniques et organisationnelles

Confidentialité

- **Contrôle des entrées:** protection contre les accès non autorisés aux installations de traitement des données: clés, cartes d'accès, gâche électrique;
- **Contrôle des accès**: protection contre les utilisations non autorisées du système: mots de passe (avec une politique correspondante), mécanismes de verrouillage automatiques, cryptage des supports de données;
- **Contrôle des autorisations**: pas de lecture, de copie, de modification ou de suppression non autorisées au sein du système: profils d'autorisation standard sur la base du «besoin d'en connaître», processus standard pour l'attribution des autorisations, vérification périodique des autorisations attribuées, en particulier des comptes utilisateur d'administrateur;
- **Pseudonymisation**: si cela est possible pour le traitement des données concerné, les identifiants primaires des données à caractère personnel sont supprimés dans l'application de données concernée et conservés séparément.
- **Schéma de classification pour les données:** sur la base des obligations légales ou d'une auto-évaluation (secret/confidentiel/interne/public).

Intégrité

- **Contrôle de la transmission**: pas de lecture, copie, modification ou suppression non autorisées lors de la transmission électronique ou du transport: cryptage, réseau virtuel privé (VPN);
- **Contrôle des saisies**: détermination de si et par qui des données à caractère personnel ont été saisies dans, modifiées ou supprimées des systèmes de traitement des données: archivage, gestion des documents;

Disponibilité et résilience

- **Contrôle de la disponibilité**: protection contre une destruction ou une perte fortuite ou délibérée: stratégie de sauvegarde (en ligne/hors ligne; sur site/hors site), alimentation sans interruption (ASI, groupe électrogène diesel), protection anti-virus, pare-feu, canaux de signalement et plans d'urgence; contrôles de sécurité au niveau de l'infrastructure et de l'application, concept de sauvegarde sur plusieurs niveaux avec externalisation des sauvegardes cryptées dans un centre de données de sauvegarde, processus standard en cas de changement/de fin de contrat des employés;
- Possibilité de **récupération rapide**;
- **Délais avant effacement**: aussi bien pour les données elles-mêmes que pour les métadonnées telles que les fichiers journaux et autres.

Procédures de vérification, d'analyse et d'évaluation régulières

- Gestion de la protection des données, y compris formations régulières des employés;
- Gestion des réponses aux incidents;
- Paramètres respectueux de la vie privée;
- **Contrôle des sous-traitants:** pas de traitement des données en sous-traitance au sens de l'art. 28 du RGPD sans instruction correspondante du Donneur d'ordre, par ex.: conception claire du contrat, gestion formalisée des missions, sélection stricte du sous-traitant (certification ISO, ISMS), obligation de conviction préalable, contrôles ultérieurs.

Annexe 5

Sous-traitants ultérieurs

Pour le traitement des données pour le compte du Donneur d'ordre, le Mandataire a recours à des prestations de tiers qui traitent des données pour son compte («Sous-traitants ultérieurs»).

Il s'agit de l'entreprise/des entreprises suivante(s):

1. Télémaintenance et assistance Easyrent par:

   WINTERSTEIGER Sports GmbH
   Wintersteigerstrasse 1
   4910 Ried im Innkreis
   Autriche

2. Réservation en ligne / Enregistrement (hébergement) Easyrent par:

   WINTERSTEIGER Sports GmbH
   Wintersteigerstrasse 1
   4910 Ried im Innkreis
   Autriche