Convention concernant la sous-traitance selon le RGPD

entre

.....

- responsable du traitement - ci-après dénommé le donneur d'ordre -

et

ALSO Suisse SA

- sous-traitant - ci-après dénommé le contractant -

1. Objet et durée du mandat

(1) Objet

L'objet du mandat pour l'utilisation des données est la réalisation des tâches suivantes par le contractant: assistance technique, traitement des tâches, prestations informatiques, service clients, services cloud conformément au contrat de produits, de prestations de service, de vente et/ou d'ouvrage correspondant.

(2) Durée

La durée du présent mandat (durée) correspond à la durée de la convention de prestations conformément au contrat de produits, de prestations de service, de vente et/ou d'ouvrage concerné.

2. Concrétisation de la teneur du mandat

(1) Nature et but du traitement de données prévu
La nature et le but du traitement de données à caractère personnel par le sous-traitant pour le donneur d'ordre résultent concrètement de la relation contractuelle établie et repose sur les CGV et d'éventuels contrats individuels et leurs annexes, ainsi que

Nature du traitement de données	But du traitement de données
Service cloud / service à distance	traitement des tâches, assistance technique, prestations informatiques, service clients, services cloud

L'exécution du traitement de données convenu contractuellement a lieu exclusivement en Suisse ou dans un État membre de l'Union européenne ou dans un autre État partie à l'accord sur l'Espace économique européen ou dans un pays pour lequel il existe une décision adéquate de la Commission européenne ou du Préposé fédéral à la protection des données et à la transparence.

(2) Nature des données

☐La nature des données personnelles utilisées est déterminée conformément à la présente relation contractuelle.

ou

☐ les types/catégories de données suivants constituent l'objet du traitement des données à caractère personnel (énumération/description des catégories de données)

☐ données de base des personnes

☐ coordonnées (par ex. téléphone, e-mail)

☐ données de base du contrat (relation contractuelle, intérêts contractuels ou pour le produit)

☐ historique du client

☐ données de facturation et de paiement du contrat

☐données de planification et de contrôle

☐ renseignements donnés (par des tiers, par ex. des sociétés de renseignement ou des répertoires publics)

☐.....

(3) Catégories de personnes concernées

Les catégories de personnes concernées par le traitement comprennent:

☐ Les catégories de personnes concernées par le traitement comprennent:

- ☐ les collaborateurs du donneur d'ordre
- ☐ les fournisseurs du donneur d'ordre
- ☐ les clients du donneur d'ordre
- ☐ les intéressés
- ☐ les agents commerciaux/revendeurs
- ☐ les interlocuteurs
- ☐ ……

3. Mesures techniques et organisationnelles

(1) le contractant doit documenter la mise en œuvre des mesures techniques et organisationnelles exposées par le donneur d'ordre avant l'attribution du mandat et nécessaires avant le commencement du traitement, en particulier en ce qui concerne l'exécution concrète du mandat et doit les transmettre au donneur d'ordre pour vérification. [Le contractant garantit la sécurité des données conformément aux mesures techniques et organisationnelles selon l'annexe 1, qui correspondent aux directives conformément à l'art. 28 al. 3 let. c, 32 RGPD notamment en liaison avec l'art. 5 al. 1, al. 2 RGPD.] En cas d'acceptation par le donneur d'ordre, les mesures techniques et organisationnelles documentées deviennent le fondement du mandat. Dans la mesure où la vérification/un audit du donneur d'ordre entraîne un besoin d'adaptation, celui-ci doit être appliqué à l'amiable. Les coûts y relatifs sont à la charge du donneur d'ordre.

Les mesures techniques et organisationnelles doivent garantir un niveau de protection adapté au risque en ce qui concerne la confidentialité, l'intégrité, la disponibilité et la capacité de résistance des systèmes. Dans ce cadre, il faut tenir compte de l'état de la technique, des coûts de mise en œuvre et de la façon, de la portée et des finalités du traitement ainsi que des différentes probabilités de

survenance et de la gravité des risques pour les droits et libertés des personnes physiques au sens de l'art. 32 al. 1 RGPD [détails à l'annexe 1].
(3) Les mesures techniques et organisationnelles sont soumises au progrès technique et au développement. Dans la mesure où il est possible au contractant de mettre en œuvre des mesures alternatives adéquates. Dans ce cadre, le niveau de sécurité ne peut pas être inférieur aux mesures fixées. Les modifications importantes sont documentées.

4. Correction, limitation et suppression des données personnelles

(1) Le contractant ne peut pas corriger, supprimer ni limité le traitement des données traitées dans le cadre du mandat de son propre chef, mais uniquement sur instruction documentée du donneur d'ordre. Dans la mesure où une personne concernée s'adresse directement au contractant à ce sujet, le contractant transmettra immédiatement cette requête au donneur d'ordre, s'il est évident pour le contractant que le client doit être attribué au donneur d'ordre.
(2) Le plan d'effacement, le droit à l'oubli, la correction, la portabilité des données et les renseignements selon les instructions documentées du donneur d'ordre sont exécutés par le contractant en tant que prestation distincte payante pour le donneur d'ordre. .

5. Assurance qualité et autres devoirs du contractant

Le contractant doit, outre le respect des règles du présent mandat, satisfaire à des obligations légales conformément aux art. 28 à 33 RGPD; il garantit en particulier le respect des prescriptions suivantes:

a) Le contractant a désigné un chargé de la protection des données. Ses coordonnées actuelles sont indiquées sur la page d'accueil du contractant de façon à être facilement accessibles.
b) Le contractant garantit la préservation de la confidentialité sur la base de la convention de confidentialité signée entre les parties ou conformément aux art. 28 al. 3 p. 2 let.b, 29, 32 al. 4 RGPD. Le contractant n'a recours lors de la réalisation des travaux qu'à des employés qui s'engagent à respecter la confidentialité et ayant été préalablement familiarisés avec les dispositions concernant la protection des données pertinentes pour eux. Le contractant et toute personne sous ses ordres ayant accès à des données à caractère personnel peuvent traiter ces données uniquement conformément aux instructions du donneur d'ordre, y compris les attributions consenties dans le présent contrat, à moins qu'ils ne soient légalement tenus de les traiter.
c) Le contractant garantit la mise en œuvre et le respect des mesures techniques et organisationnelles conformément à l'art. 28 al. 3 p. 2 let. c, 32 RGPD [Détails dans l'annexe 1 « mesures techniques et organisationnelles »].
d) Le donneur d'ordre et le contractant collaborent sur demande avec les autorités de surveillance lors de l'accomplissement de leur mission.
e) L'information immédiate du donneur d'ordre au sujet des contrôles et des mesures de l'autorité de surveillance dans la mesure où elles se rapportent au présent mandat. Cela s'applique aussi dans la mesure où une autorité responsable enquête, dans le cadre d'une procédure d'infraction administrative ou pénale concernant le traitement des données à caractère personnel lors de la sous-traitance chez le contractant.
f) Dans la mesure où le donneur d'ordre fait l'objet pour sa part d'un contrôle de l'autorité de surveillance, d'une procédure administrative ou pénale, d'une revendication de

responsabilité par une personne concernée ou un tiers ou d'une autre revendication en lien avec la sous-traitance chez le contractant, le contractant doit l'aider de son mieux.

g) Le contractant contrôle régulièrement les procédures internes ainsi que les mesures techniques et organisationnelles pour garantir que le traitement sous sa responsabilité est effectué conformément aux exigences de la législation sur la protection des données en vigueur et que la protection des droits de la personne concernée est garantie en fonction du risque.

h) Le contractant prouve que les mesures techniques et organisationnelles ont été prises vis-à-vis du donneur d'ordre dans le cadre de ses pouvoirs de contrôle en vertu du chiffre 7 du présent contrat.

6. Relations de sous-traitance

(1) Les prestations de services qui se rapportent directement à l'exécution de la prestation principale doivent être considérées comme des relations de sous-traitance au sens du présent règlement. Les prestations accessoires auxquelles le contractant recourt, par ex. des services de télécommunication, des services postaux/de transport, des services de maintenance et à la clientèle ou l'élimination de supports de données ainsi que d'autres mesures pour garantir la confidentialité, la disponibilité, l'intégrité et la capacité de résistance du matériel informatique et des logiciels des installations de traitement des données, n'en font pas partie. Le contractant est toutefois tenu, pour garantir la protection des données et la sécurité des données du donneur d'ordre, également en cas de prestations accessoires délocalisées, de passer des dispositions contractuelles appropriées et conformes à la législation, et de prendre des mesures de contrôle.

(2) Le donneur d'ordre accorde par la présente convention une autorisation générale pour que le contractant puisse stocker des données également dans un pays tiers s'il existe un niveau équivalent de protection des données ou qu'il est établi par une garantie appropriée, notamment par l'utilisation des clauses standard de l'UE sur la protection des données. Le contractant informe le donneur d'ordre de toute modification envisagée concernant l'ajout ou le remplacement d'autres sous-traitants ce qui permet au donneur d'ordre de s'opposer à des modifications de ce type en donnant les raisons dans un délai de 14 jours à partir de la communication, sinon la sous-traitance est considérée comme approuvée. L'information du donneur d'ordre s'effectue par [publication sur le site Web du contractant ou par envoi d'un e-mail]. En cas d'opposition du donneur d'ordre et si le choix d'un autre sous-traitant n'est pas possible, le donneur d'ordre peut exceptionnellement mettre un terme à la relation contractuelle sans aucun droit de remboursement.

(3) Le contractant sélectionnera avec soin des sous-traitants selon leurs aptitudes, en particulier les exigences du RGPD, et effectuera des contrôles réguliers. La transmission de données à caractère personnel du donneur d'ordre vers les sous-traitants et la première intervention de ceux-ci ne sont autorisées qu'à partir du moment où toutes les conditions pour une sous-traitance sont remplies. L'ensemble des dispositions contractuelles dans la chaîne contractuelle doivent être imposées aux autres sous-traitants.

7. Droits de contrôle du donneur d'ordre

(1) Le donneur d'ordre a le droit, en commun accord avec le contractant, de vérifier les prestations conformément à l'étendue des prestations du contrat principal ou de faire effectuer des vérifications par un contrôleur soumis au secret professionnel ou à désigner au cas par cas une fois par an pendant

2 jours au maximum durant les heures habituelles de bureau (audit). Il a le droit de s'assurer, par des contrôles par sondage, qui en règle générale doivent être notifiés au moins 10 jours à l'avance, du respect de la présente convention par le contractant dans son activité commerciale.

(2)La preuve du respect des mesures techniques et organisationnelles qui ne concernent pas uniquement le mandat concret, peut être faite par le respect de règles de conduite approuvées conformément à l'art. 40 RGP, la certification d'après un processus de certification agréé conformément à l'art. 42 RGPD, des attestations récentes, des rapports ou des extraits de rapport, des audits par des instances indépendantes (p. ex. un commissaire aux comptes, une révision, un chargé de la protection des données, le département sécurité informatique, des auditeurs de la protection des données, des auditeurs qualité) ou une certification appropriée par l'audit de sécurité informatique ou de protection des données

(4) pour permettre la réalisation de contrôles par le donneur d'ordre, le contractant peut faire valoir un droit à rémunération.

8. Communication en cas de manquements de la part du contractant

(1) Le contractant apporte son soutien au donneur d'ordre concernant le respect des obligations mentionnées dans les art. 32 à 36 du RGPD en matière de sécurité des données à caractère personnel, les obligations de déclaration en cas de pannes et de pertes de données, les évaluations d'impact de la protection des données et les consultations préalables, qui comprennent entre autres

a) l'obligation de signaler au donneur d'ordre les violations de données à caractère personnel dans un délai de 48 heures à compter de la découverte de celles-ci
b) l'obligation de soutenir le donneur d'ordre dans le cadre de son devoir d'information vis-à-vis des personnes concernées et, dans ce contexte, de mettre immédiatement à disposition de celui-ci l'ensemble des informations pertinentes
c) le soutien du donneur d'ordre pour son évaluation d'impact de la protection des données; et
d) le soutien du donneur d'ordre dans le cadre de consultations préalables avec l'autorité de surveillance.

(2) pour les services d'assistance qui ne font pas partie du cahier des charges ou qui ne sont pas imputables à un manquement du contractant, le contractant peut demander une rémunération.

9. Autorité du donneur d'ordre

(1) Le donneur d'ordre confirme les instructions orales sans délai par écrit. Tant qu'aucune confirmation écrite n'est présentée le contractant peut attendre pour exécuter les instructions.

(2) Le contractant doit informer sans délai le donneur d'ordre lorsqu'il est d'avis qu'une instruction enfreint des dispositions de protection des données. Le contractant est habilité à suspendre la réalisation des instructions correspondantes jusqu'à ce qu'elles soient confirmées ou modifiées par le donneur d'ordre.

10. Suppression et restitution de données à caractère personnel

(1) Des copies ou des duplicatas des données ne sont pas établis sans que le donneur d'ordre en ait connaissance. Les copies de sécurité, dans la mesure où elles sont nécessaires à la garantie du bon

traitement des données, ainsi que les données nécessaires en vue de respecter des obligations légales de conservation ne sont pas concernées par ce point.
(2) Après la clôture des travaux convenus contractuellement ou plus tôt sur instruction du donneur d'ordre (au plus tard à l'expiration de l'accord de niveau de service), le contractant doit remettre au donneur d'ordre l'ensemble des documents étant entrés en sa possession, des résultats de traitement et d'utilisation créés ainsi que les bases de données qui sont en lien avec le mandat spécifique, ou, après accord préalable, les détruire irrévocablement dans le mesure où cela est techniquement possible. Il en va de même pour les documents de tests et à jeter. Le protocole de l'effacement doit être produit sur demande.
(3) Les documentations et correspondances servant de preuve au bon traitement des données conformément au mandat doivent être conservées par le contractant conformément aux délais de conservation correspondants après l'échéance du contrat.

_____, le _____ _____, le _____

Donneur d'ordre: **Contractant:**

_____ _____

(signature / cachet de l'entreprise) (signature / cachet de l'entreprise)

_____ _____

(fonction du signataire) (fonction du signataire)

_____ _____

(nom du signataire en caractères d'imprimerie) (nom du signataire en caractères d'imprimerie)

Annexe 1 – Mesures techniques et organisationnelles

1. Confidentialité (convention de confidentialité/déclaration de protection des données du ... / art. 32 al. 1 lettre b RGPD)

- Contrôle de l'accès
  Aucun accès non autorisé aux installations de traitement des données, les mesures minimales

sont par ex.: des cartes magnétiques ou à puce, des clefs, des gâches électriques, un gardien ou portier, des alarmes et/ou des installations vidéo;

- Contrôle de l'accès
  Aucune utilisation non autorisée du système, par ex.: des mots de passe (sûrs et imposés), des mécanismes de blocage automatiques, une authentification à deux facteurs, le cryptage des supports de données;
- Contrôle de l'accès
  Aucune lecture, copie, modification ou suppression non autorisée au sein du système, par ex.: Concepts d'autorisation et droits d'accès adaptés aux besoins, journalisation des accès;
- Contrôles de la ségrégation
  Le traitement séparé de données qui ont été collectées à des fins différentes, par ex. multi-mandants, sandboxing;
- Pseudonymisation (art. 32 al. 1 lettre a RGPD; art. 25 al. 1 RGPD)
  Le traitement des données à caractère personnel de façon telle que les données ne puissent plus être associées à une personne concernée spécifique sans consulter des informations supplémentaires, dans la mesure où ces informations supplémentaires sont conservées séparément et sont soumises aux mesures techniques et organisationnelles appropriées;
- Cryptage

2. Intégrité (analogue à l'art. 32 al. 1 lettre b RGPD)

- Contrôle de la transmission
  Aucune lecture, copie, modification ou suppression non autorisée lors de la transmission électronique ou du transport, par ex.: cryptage, Virtual Private Networks (VPN), signature électronique;
- Contrôle des entrées
  Identification de l'entrée, la modification et la suppression de données à caractère personnel dans le système de traitement des données ainsi que de la personne l'ayant effectué, par ex.: journalisation, gestion documentaire;

3. Disponibilité et capacité de résistance (art. 32 al. 1 lettre b RGPD)

- Contrôle de la disponibilité
  Protection contre la destruction accidentelle ou volontaire ou la perte, par ex.: Stratégie de back-up (en ligne/hors ligne; sur site/hors site), source d'alimentation non interruptible (ASC), protection anti-virus, firewall, voies de communication et plans d'urgence;
- Récupération rapide (analogue à l'art. 32 al. 1 lettre b RGPD)

4. Procédure pour le contrôle, l'appréciation et l'évaluation réguliers (analogue à l'art. 32 al. 1 lettre b RGPD; art. 25 al. 1 RGPD)

- Gestion de la protection des données;
- Incident-Response-Management;
- Protection des données par défaut (art. 25 al. 2 RGPD);
- Contrôle du traitement des données assuré par des tiers
  Pas de traitement de données en sous-traitance au sens de l'art. 28 RGPD sans instruction correspondante du donneur d'ordre, par ex.: présentation univoque du contrat, gestion du contrat formalisée, choix strict des prestataires de services, devoir de due diligence, contrôles a posteriori.