Convention de sous-traitance

entre

ALSO Suisse SA

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

et

.....

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

1. Objet et durée du mandat

(1) Objet

☐ L'objet du mandat découle de l'accord de niveau de service/SLA/..... du....., auquel il est fait référence dans les présentes (ci-après l'accord de niveau de service).

ou

☐ L'objet du mandat pour l'utilisation des données est la réalisation des tâches suivantes par le contractant: …… (définition des tâches)

(2) Durée

☐ La durée du présent mandat (durée) correspond à la durée de l'accord de niveau de service.

ou *(en particulier au cas où il n'y a pas d'accord de niveau de service pour la durée)*

☐ Le mandat est accordé pour une mise en œuvre unique.

ou

☐ La durée du présent mandat (durée) est limitée jusqu'au .....

ou

☐ Le mandat est accordé de façon illimitée et peut être résilié par les deux parties moyennant un préavis de ..... à ....., sans préjudice de la possibilité de résiliation sans préavis.

2. Concrétisation de la teneur du mandat

(1) Nature et but du traitement de données prévu

☐ La nature et le but du traitement des données à caractère personnel par le contractant pour le donneur d'ordre sont décrits concrètement dans l'accord de niveau de service du .....

ou

☐ Description plus précise de l'objet du mandat en ce qui concerne la nature et le but des tâches du contractant: .....

L'exécution du traitement de données convenu contractuellement est effectuée 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. Une communication transfrontalière des données vers un État tiers ne disposant de législation correspondante assurant un niveau de protection adéquat n'est en principe pas autorisée d'après l'art. 6 al. 1 LPD. Dans de tels cas, une communication de données transfrontalière ne peut avoir lieu que si les conditions juridiques de l'art. 6 al. 1 et 2 LPD sont remplies et conformément à la liste des États réputés offrir une législation sur la protection des données appropriée d'après l'art. 7.

Dans la mesure où la loi européenne sur la protection des données entre en application, tout stockage dans un pays tiers nécessite l'accord préalable du donneur d'ordre et ne peut être réalisé que si les conditions juridiques spécifiques de l'art. 44 et suivants RGPD sont remplies.

☐ est constaté par une décision de la Commission constatant son caractère adéquat (art. 45 al. 3 RGPD);

☐ est établi par des dispositions de protection des données internes contraignantes (art. 46 al. 2 lettre b en lien avec art. 47 RGPD);

☐ est établi par des clauses standard sur la protection des données (art. 46 al. 2 lettres c et d RGPD);

☐ est établi par des règles de conduite approuvées (art. 46 al. 2 lettre e en lien avec art. 40 RGPD);

☐ est établi par un mécanisme de certification agréé (art. 46 al. 2 lettre f en lien avec art. 42 RGPD);

☐ est établi par d'autres mesures: …… (Art. 46 al. 2 lettre a, al. 3 lettres a et b RGPD).

(2) Nature des données

☐ La nature des données à caractère personnel utilisées est décrite concrètement dans l'accord de niveau de service à la section: .....

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)

☐.....

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

☐ les données sur l'origine raciale et ethnique (par ex. photo dans le dossier personnel)

☐ les opinions politiques, les convictions religieuses ou philosophiques ou les activités

☐ l'appartenance à un syndicat

☐ les données génétiques

☐ les données biométriques pour l'identification univoque d'une personne physique

☐ les données relatives à la santé

☐ les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique

☐ des mesures d'aide sociale

☐ des poursuites et sanctions administratives ou pénales

(3) Catégories de personnes concernées

☐ Les catégories de personnes concernées par le traitement sont décrites concrètement dans l'accord de niveau de service à la section: .....

ou

☐ Les catégories de personnes concernées par le traitement comprennent:

☐ les clients

☐ les clients potentiels

☐ les intéressés

☐ les abonnés

☐ les collaborateurs

☐ les fournisseurs

☐ les agents commerciaux/revendeurs

☐ les interlocuteurs

☐ les utilisateurs Internet

☐ les actionnaires (pour les sociétés anonymes ouvertes au public)

☐ …

3. Mesures techniques et organisationnelles

(1) le contractant doit documenter la mise en œuvre des mesures techniques et organisationnelles exposées 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. En cas d'acceptation par le donneur d'ordre, les mesures 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.
(2) Le contractant doit garantir les mesures techniques et organisationnelles conformément à l'art. 7 LPD en lien avec les art. 8 à 12 OLPD. Pour les données ayant des points de contact avec l'UE, des sécurités doivent être établies conformément à l'art. 28 al. 3 lettre c, 32 RGPD, en particulier en lien avec l'art. 5 al. 1, al. 2 RGPD. Globalement, les mesures à prendre sont des mesures concernant la sécurité des données et la garantie d'un niveau de protection adapté au risque en ce qui concerne la confidentialité, l'intégrité, la disponibilité et la capacité de charge du système. 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 et à l'évolution techniques. 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 doivent être documentées.

4. Correction, limitation et suppression des données

(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 (conformément à l'art. 5 LPD en lien avec l'art. 8 LPD), le contractant transmettra immédiatement cette requête 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 doivent être garantis par le contractant. Le contractant garantit en outre de soutenir le donneur d'ordre pour satisfaire les droits des personnes concernées et de prendre des mesures appropriées dans la mesure où les demandes se répètent. .

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 à aux art. 4 à 12 OLPD et des art. 28 à 33 RGPD; il garantit en particulier le respect des prescriptions suivantes: [Veuillez cocher et remplir les éléments applicables:]

a) ☐ commande écrite d'un chargé de la protection des données qui exerce ses activités conformément aux art. 38 et 39 RGPD.

☐ Ses coordonnées seront transmises au donneur d'ordre aux fins d'une prise de contact directe. Tout changement de chargé de la protection des données sera communiqué immédiatement au donneur d'ordre.

☐Monsieur/Madame [insérer: prénom, nom, unité administrative, téléphone, e-mail]

.....
.....
.....

..... est désigné en tant que chargé de la protection des données chez le contractant. Tout changement de chargé de la protection des données doit être communiqué immédiatement au donneur d'ordre.

☐ Ses coordonnées actuelles sont indiquées sur la page d'accueil du contractant de façon à être facilement accessibles.

b) ☐ Le contractant n'est pas tenu de désigner un chargé de la protection des données. Monsieur/Madame [insérer: prénom, nom, unité administrative, téléphone, e-mail] ..... est nommé personne de contact chez le contractant.

c) ☐ Étant donné que le contractant a son siège en dehors de l'Union, il nomme le représentant suivant dans l'Union conformément à l'art. 27 al. 1 RGPD: [insérer: prénom, nom, unité administrative, téléphone, e-mail] .....

d) ☐ Le contractant, qui a son siège en dehors de l'Union, n'est pas tenu de nommer un représentant dans l'Union conformément à l'art. 27 al. 1 RGPD.

e) ☐ 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 lettre 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 les ordres du contractant qui ont 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.

f) ☐ Le contractant garantit la mise en œuvre et le respect de toutes les mesures techniques et organisationnelles nécessaires au présent mandat conformément aux art. 8 à 12 OLPD ou à l'art. 28 al. 3 p. 2 lettre c, 32 RGPD. 1 LPD [détails à l'annexe 1 «Mesures techniques et organisationnelles»].

g) ☐ Le donneur d'ordre et le contractant collaborent sur demande avec les autorités de surveillance lors de l'accomplissement de leur mission.

h) ☐ 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.

i) ☐ 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.

j) ☐ 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 des personnes concernées est garantie.

k) ☐ La possibilité de prouver 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.

l) ☐ Le contractant consigne le traitement automatisé des données à caractère personnel sensibles ou des profils de la personnalité conformément à l'art. 10 OLPD.

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 contractant peut charger des sous-traitants (d'autres sous-traitant) uniquement après accord écrit ou documenté exprès préalable du donneur d'ordre.

a) ☒ Une sous-traitance est interdite.

b) ☐ Le donneur d'ordre approuve la délégation aux sous-traitants suivants à condition qu'un accord contractuel soit conclu conformément à l'art. 10a LPD ou à l'art. 28 al. 2-4 RGPD:

Société sous-traitant	adresse postale/pays	Prestation	Catégories de données traitées

c) ☐ la décentralisation vers des sous-traitants ou

☐ le changement du sous-traitant existant

sont autorisés, dans la mesure où:

- le contractant annonce préalablement ladite décentralisation vers des sous-traitants au donneur d'ordre par écrit ou sous forme écrite avec un délai de préavis approprié et

- que le donneur d'ordre n'émet pas d'objection écrite ou sous forme écrite vis-à-vis du contractant quant à la décentralisation prévue jusqu'au moment de la transmission des données et
- qu'un accord contractuel conformément à l'art. 10a LPD ou à l'art. 28 al. 2-4 RGPD sert de base à celui-ci.

(3) 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.
(4) Si le sous-traitant effectue les prestations convenues en dehors de la Suisse ou de l'UE/EEE, le contractant s'assurera de la recevabilité du point de vue de la législation sur la protection des données par des mesures appropriées. Il en va de même lorsqu'il faut faire appel à des prestataires de services au sens de l'al. 1 phrase 2.
(5) Une décentralisation supplémentaire par le sous-traitant

☒ n'est pas autorisée;
☐ nécessite l'accord exprès du donneur d'ordre principal (au moins sous forme écrite);
☐ nécessite l'accord exprès du contractant principal (au moins sous forme écrite);

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, d'un commun accord avec le contractant, de faire effectuer des vérifications par un contrôleur soumis au secret professionnel ou à désigner au cas par cas (audit). Il a le droit de s'assurer, par des contrôles par sondage, qui en règle générale doivent être notifiés en temps voulu, du respect de la présente convention par le contractant dans son activité commerciale.
(2) Le contractant s'assure que le donneur d'ordre est en mesure de s'assurer du respect des devoirs du contractant conformément à l'art. 10 LPD et à l'art. 28 RGPD. Le contractant s'engage à fournir sur demande au donneur d'ordre les renseignements exigés et en particulier à prouver la mise en œuvre des mesures techniques et organisationnelles.
(3) La preuve de ces mesures qui ne concernent pas uniquement le mandat concret, peut être faite par le respect des engagements convenus (la certification d'après un processus de certification agréé conformément à l'art. 11 LPD ou à l'art. 42 RGPD; des audits par des instances indépendantes (par ex. un réviseur d'entreprises, une révision, un chargé de la protection des données, le département sécurité informatique, des auditeurs de la protection des données, des auditeurs qualité); une certification appropriée par l'audit de sécurité informatique ou de protection des données (par ex. la protection de base d'après BSI).
(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 soutient le donneur d'ordre pour le respect des obligations susmentionnées 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) la garantie d'un niveau de protection approprié par des mesures techniques et organisationnelles qui tiennent compte des circonstances et des finalités du traitement ainsi que de la probabilité pronostiquée et de la gravité d'une violation potentielle de la loi par des failles de sécurité et permettent une constatation immédiate des événements de violation.
b) l'obligation de signaler immédiatement au donneur d'ordre les violations de données à caractère personnel dans un délai de 24 heures à compter de la découverte de celles-ci
c) 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
d) le soutien du donneur d'ordre pour son évaluation d'impact de la protection des données
e) 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 (au moins sous forme écrite).

(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 concernée 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 et l'effacement doit être confirmé par écrit.
(3) Les documentations 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. Il peut les transmettre au donneur d'ordre à l'échéance du contrat pour se décharger.

_____, le _____

Donneur d’ordre:

_____

_____

(signature / cachet de l'entreprise)

_____

(fonction du signataire)

_____

(nom du signataire en caractères d'imprimerie)

_____, le _____

Contractant:

_____

_____

(signature / cachet de l'entreprise)

_____

(fonction du signataire)

_____

(nom du signataire en caractères d'imprimerie)

Annexe – 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 (analogue à l'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.