

Accord de traitement de données

entre

- le Responsable de traitement – ci-après dénommé le Client -
et

ALSO France, 10 avenue des Louvresses 92230 GENNEVILLIERS

- Le Sous-traitant - ci-après dénommé le Fournisseur

1. Objet et durée de la Commande ou du Contrat

(1) Objet

L'objet de la Commande ou du Contrat concernant le traitement des données est l'exécution des services ou tâches suivants par le Fournisseur : Assistance technique, Traitement des commandes, Services informatiques, Service client, Services Cloud.

(2) Durée

La durée de cette commande (terme) correspond à la durée du contrat de service dans le cadre des contrats de produit, de service, d'achat et/ou de travail respectifs.

2. Spécification de la commande ou des détails du contrat

(1) Nature et but du traitement prévu des données

Description détaillée de l'Objet en ce qui concerne la nature et l'objet des services fournis par le fournisseur :

Nature des données	But du traitement	Sujet de données
Données personnelles : nom, adresse, coordonnées, coordonnées bancaires	Traitement des commandes, assistance technique, services informatiques, service client, services Cloud	Employés du responsable de traitement de données, partenaire commercial, client, vendeur, personnes intéressées

L'exécution du traitement des données convenu par contrat doit être effectuée exclusivement dans un État membre de l'Union européenne (UE), dans un État membre de l'Espace économique européen (EEE) ou dans un pays inclus dans la décision d'adéquation de la Commission Européenne. Chaque transfert de données à un État qui n'est pas un État membre de l'UE ou de l'EEE nécessite l'accord préalable du client et ne doit avoir lieu que si les conditions spécifiques des articles 44 et suivant du RGPD ont été remplies. Le niveau de protection adéquat dans un pays qui n'est pas membre de l'UE devrait être garanti par des clauses contractuelles types de l'UE. (Art 46 alinéa 2 point c et d du UE-RGPD)

(2) Type de données

Le Sujet du traitement des données personnelles comprend les types/catégories de données suivants : Données de base personnelles (Données personnelles clés), Données de contact, Données contractuelles clés (Relations contractuelles/juridiques, Intérêts contractuels ou produits), Historique client, Facturation contractuelle et Données de paiements, Informations divulguées (provenant de tiers, par exemple agences de référence de crédit ou d'annuaires publics), Informations sur la configuration du système et l'environnement du client.

(3) Catégories de sujets de données

Les Catégories de sujets de données comprennent : les employés du responsable de traitement de données, le partenaire commercial, les clients, les clients potentiels, les abonnés, les employés, les fournisseurs et les personnes à contacter.

3. Mesures techniques et organisationnelles

(1) Avant le début du traitement, le Fournisseur doit documenter l'exécution des Mesures techniques et organisationnelles nécessaires, définies avant l'attribution de la Commande ou du Contrat, en particulier en ce qui concerne l'exécution détaillée du contrat, et présenter ces mesures documentées au Client pour contrôle. Dès acceptation par le Client, les mesures documentées deviennent la base du contrat. Dans la mesure où l'inspection/audit par le Client montre la nécessité de modifications, ces modifications doivent être mises en œuvre d'un commun accord.

(2) Le Fournisseur établit la garantie conformément à l'article 28, alinéa 3, point c, et à l'article 32 du RGPD, en particulier en liaison avec l'article 5, alinéa 1, et l'article 2 du RGPD. Les mesures à prendre sont des mesures de sécurité des données et des mesures qui garantissent un niveau de protection approprié au risque concernant la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes. L'état de la technique, les coûts de mise en œuvre, la nature, la portée et les finalités du traitement ainsi que la probabilité de survenance et la gravité du risque pour les droits et libertés des personnes physiques au sens de l'article 32, alinéa 1 du RGPD doivent être pris en compte. [détails en annexe]

(3) Les Mesures techniques et organisationnelles font l'objet de progrès techniques et de développement ultérieur. À cet égard, il est permis au Fournisseur de mettre en œuvre d'autres mesures adéquates. Ce faisant, le niveau de sécurité des mesures définies ne doit pas être réduit. Les changements substantiels doivent être documentés.

4. Rectification, restriction et effacement des données

(1) Le Fournisseur ne peut, de sa propre autorité, rectifier, effacer ou restreindre le traitement des données traitées pour le compte du Client, mais uniquement sur instructions documentées du Client. Dans la mesure où un Sujet de données contacte directement le Fournisseur au sujet d'une rectification, d'un effacement ou d'une restriction du traitement, le Fournisseur transmettra immédiatement la demande du sujet de données au Client.

(2) Dans la mesure où il est inclus dans la portée des services, la politique d'effacement, le « droit à l'oubli », la rectification, la portabilité des données et l'accès doivent être assurés par le Fournisseur conformément aux instructions documentées du Client sans retard injustifié.

5. Assurance qualité et autres devoirs du Fournisseur

En plus de se conformer aux règles énoncées dans la présente Commande ou le Contrat, le Fournisseur doit se conformer aux exigences légales visées aux articles 28 à 33 du RGPD ; en conséquence, le Fournisseur assure notamment le respect des exigences suivantes :

- a) Désigner un Délégué à la protection des données, qui exerce ses fonctions conformément aux articles 38 et 39 du RGPD.
- b) Confidentialité conformément à l'article 28, alinéa 3, phrase 2, point b, articles 29 et 32, alinéa 4, du RGPD. Le Fournisseur confie uniquement aux employés le traitement des données décrit dans ce Contrat, qui ont été liés à la confidentialité et ont déjà été familiarisés avec les dispositions relatives à la protection des données relatives à leur travail. Le Fournisseur et toute personne agissant sous son autorité qui a accès aux données personnelles, ne doivent traiter ces données que sur les instructions du Client, qui inclut les pouvoirs accordés dans le présent contrat sauf si la loi l'exige.
- c) Mise en œuvre et respect de toutes les Mesures techniques et organisationnelles nécessaires pour la présente Commande ou le Contrat, conformément à l'article 28, alinéa 3, phrase 2, point c, article 32 du RGPD [détails en annexe].
- d) Le Client et le Fournisseur coopèrent, sur demande, avec l'autorité de surveillance dans l'exécution de ses tâches.
- e) Le Client doit être informé immédiatement de toutes les inspections et mesures effectuées par l'autorité de surveillance, dans la mesure où elles concernent la présente Commande ou le Contrat. Ceci s'applique également dans la mesure où le Fournisseur fait l'objet d'une enquête ou participe à une enquête par une autorité compétente en rapport avec des infractions à toute loi civile ou pénale, ou toute règle administrative ou règlement concernant le traitement des données personnelles dans le cadre du traitement de cette Commande ou Contrat.
- f) Dans la mesure où le Client est soumis à une inspection par l'autorité de contrôle, une infraction administrative ou sommaire ou une procédure pénale, une réclamation de responsabilité par un Sujet de données ou par un tiers ou toute autre réclamation relative à la Commande ou au Fournisseur, le Fournisseur fera tout son possible pour soutenir le Client.
- g) Le Fournisseur surveille périodiquement les processus internes et les mesures techniques et organisationnelles pour s'assurer que le traitement dans son domaine de responsabilité est conforme aux exigences de la loi applicable sur la protection des données et à la protection des droits de la personne concernée.
- h) Vérifiabilité des mesures techniques et organisationnelles réalisées par le Client dans le cadre des pouvoirs de surveillance du Client visés à l'article 7 du présent contrat.

6. Sous-traitant

(1) La sous-traitance aux fins du présent Accord doit être comprise comme signifiant les services qui se rapportent directement à la fourniture du service principal. Cela n'inclut pas les services auxiliaires, tels que les services de télécommunication, les services postaux/de transport, les services de maintenance et de support aux utilisateurs ou l'élimination des supports de données, ainsi que d'autres mesures pour garantir la confidentialité, la disponibilité, l'intégrité et la résilience de l'équipement de traitement de données (hardware et software). Le Fournisseur est toutefois tenu de prendre des dispositions contractuelles appropriées et juridiquement contraignantes et de prendre les mesures d'inspection appropriées pour assurer la protection des données et la sécurité des données du Client, même dans le cas de services auxiliaires externalisés.

(2) Les commandes peuvent être transmises à des sous-traitants dans le cadre des activités convenues dans la commande. Les sous-traitants seront notifiés au client sur demande. Le Fournisseur sélectionnera soigneusement les sous-traitants en fonction de leur adéquation, en particulier en ce qui concerne les exigences de l'UE-RGPD, et les inspectera régulièrement. En outre, le Fournisseur doit convenir avec les sous-traitants d'un accord sur le traitement des commandes conformément à cet accord.

(3) Le transfert des données personnelles du Client au sous-traitant et le début du traitement des données par les sous-traitants ne doivent être entrepris qu'après avoir satisfait à toutes les exigences.

(4) Si le sous-traitant fournit le service convenu en dehors de l'UE, le Fournisseur doit garantir le respect des Règles de protection des données de l'UE par des mesures appropriées. Il en va de même si les prestataires de services doivent être utilisés au sens de l'alinéa 1 phrase 2.

(5) L'externalisation supplémentaire par le sous-traitant nécessite le consentement fournisseur (au moins sous forme de texte). Toutes les règles contractuelles de la chaîne contractuelle doivent également être imposées à l'autre sous-traitant.

7. Pouvoirs de surveillance du Client

(1) Le Client a le droit, après consultation du Fournisseur, de procéder à des inspections par une personne tenue au secret professionnel ou de les faire effectuer par un auditeur désigné au cas par cas. Afin de s'assurer du respect de cet accord par le Fournisseur dans ses opérations commerciales il pourra réaliser des contrôles aléatoires qui devront être annoncés en temps utile.

(2) Le Fournisseur doit s'assurer que le Client est en mesure de vérifier le respect des obligations du Fournisseur conformément à l'article 28 du RGPD. Le Fournisseur s'engage à fournir au Client les informations nécessaires sur demande et en particulier, à démontrer l'exécution des Mesures techniques et organisationnelles.

(3) La preuve de telles mesures, qui concernent non seulement la Commande ou le Contrat spécifique, peut être fournie par le respect des Codes de conduite approuvés conformément à l'article 40 du RGPD ; la Certification selon une procédure de certification approuvée conformément à l'article 42 du RGPD ; les Certificats d'audit, rapports ou extraits de rapports d'audit fournis par des organismes indépendants (par exemple, auditeur, Délégué à la protection des données, service de sécurité informatique, auditeur de la confidentialité des données, auditeur qualité). Une certification appropriée par la sécurité informatique ou l'audit de protection des données (par exemple, selon BSI-Grundschutz, certification IT Baseline Protection développée par l'Office fédéral allemand de la sécurité informatique (BSI) ou ISO/IEC 27001).

(4) Le Fournisseur peut réclamer une rémunération pour les inspections du Client.

8. Communication en cas d'infraction par le Fournisseur

(1) Le Fournisseur assistera le Client dans le respect des obligations relatives à la sécurité des données personnelles, aux exigences de déclaration des violations de données, aux études d'impact sur la protection des données et aux consultations préalables, visées aux articles 32 à 36 du RGPD. Ceux-ci comprennent :

- a) L'Assurance d'un niveau approprié de protection par des Mesures techniques et organisationnelles qui tiennent compte des circonstances et des objectifs du traitement ainsi que de la probabilité et de la gravité projetées d'une éventuelle violation de la loi en raison de vulnérabilités de sécurité et qui permettent une détection immédiate des infractions pertinentes.
- b) L'obligation de signaler immédiatement une violation de données personnelles au Client.
- c) Le devoir d'assister le Client en ce qui concerne l'obligation du Client de fournir des informations au Sujet de données et de fournir immédiatement au Client toutes les informations pertinentes à cet égard.
- d) Soutenir le Client dans son évaluation de l'impact de la protection des données.
- e) Soutenir le Client en ce qui concerne la consultation préalable de l'autorité de surveillance.

(2) Le Fournisseur peut réclamer une compensation pour les services d'assistance qui ne sont pas inclus dans la description des services et qui ne sont pas attribuables à des défaillances de la part du Fournisseur.

9. Autorité du Client pour donner des instructions

- (1) Le Client doit immédiatement confirmer les instructions orales (au minimum sous forme de texte).
- (2) Le Fournisseur doit immédiatement informer le Client s'il considère qu'une instruction enfreint les Règles de protection des données. Le Fournisseur aura alors le droit de suspendre l'exécution des instructions pertinentes jusqu'à ce que le Client les confirme ou les modifie.

10. Suppression et retour des données personnelles

- (1) Les copies ou duplicata des données ne doivent jamais être créés à l'insu du Client, à l'exception des copies de sauvegarde dans la mesure où elles sont nécessaires pour assurer un traitement ordonné des données, ainsi que des données requises pour respecter les exigences réglementaires de conservation des données.
- (2) Après la conclusion du contrat, ou au plus tôt à la demande du client, au plus tard à la résiliation du contrat de service, le Fournisseur cède au Client ou - sous réserve d'un accord préalable - détruit tous les documents, résultats de traitement et d'utilisation, les ensembles de données liés au Contrat qui sont entrés en sa possession, d'une manière conforme à la protection des données. Il en va de même pour tout test, déchet, matériel redondant et mis au rebut. Le journal de la destruction ou de la suppression doit être fourni sur demande.
- (3) La documentation utilisée pour démontrer le traitement ordonné des données conformément à la Commande ou au Contrat doit être conservée au-delà de la durée du contrat par le Fournisseur conformément aux périodes de conservation respectives. Il peut remettre cette documentation au Client à la fin de la durée du contrat pour décharger le Fournisseur de cette obligation contractuelle.



Client : _____

Fournisseur : _____

(Lieu/date)

(Lieu/date)

(Signature/Cachet)

(Signature/Cachet)

(Nom/fonction du signataire)

(Nom/fonction du signataire)

Annexe - Mesures techniques et organisationnelles

1. Confidentialité (Article 32 Alinéa 1 Point b du RGPD)
 - Contrôle d'accès physique
Aucun accès non autorisé aux Installations de traitement de données, par exemple : cartes magnétiques ou à puce, clés, ouvre-portes électroniques, services de sécurité d'installation et/ou personnel de sécurité d'entrée, systèmes d'alarme, systèmes vidéo/de vidéosurveillance
 - Contrôle d'accès électronique
Aucune utilisation non autorisée des Systèmes de traitement de données et de stockage de données, par exemple : mots de passe (sécurisés), mécanismes de blocage/verrouillage automatiques, authentification à deux facteurs, chiffrement des supports de données/supports de stockage
 - Contrôle d'accès interne (autorisations pour les droits d'accès et de modification des données)
Aucune lecture, copie, modification ou suppression de données non autorisée dans le système, par ex. concept d'autorisation de droits, droits d'accès basés sur les besoins, consignation des événements d'accès au système
 - Contrôle d'isolement
Traitement de données isolé, qui est collecté à des fins différentes, par ex. support client multiple, sandboxing ;
 - Pseudonymie (article 32, alinéa 1, point a), du RGPD, article 25, paragraphe 1, du RGPD)
Le traitement de données à caractère personnel de telle manière que les données ne peuvent pas être associées à un Sujet de données sans l'aide d'informations supplémentaires, à condition que ces informations supplémentaires soient stockées séparément et soumises à des Mesures techniques et organisationnelles appropriées.

2. Intégrité (Article 32 Alinéa 1 Point b du RGPD)
 - Contrôle de transfert de données
Aucune lecture, copie, modification ou suppression de données non autorisée avec transfert ou transport électronique, par exemple : cryptage, réseaux privés virtuels (VPN), signature électronique ;
 - Contrôle d'entrée de données
La vérification, si et par qui les données personnelles sont entrées dans un Système de traitement de données, est modifiée ou supprimée, par exemple : journalisation, gestion de documents

3. Disponibilité et résilience (Article 32 Alinéa 1 Point b du RGPD)
 - Contrôle de la disponibilité
Prévention de la destruction ou de la destruction accidentelle ou intentionnelle, par exemple : stratégie de sauvegarde (en ligne/hors-ligne, sur site/hors site), alimentation sans coupure, protection antivirus, pare-feu informatique, procédures de signalement et planification d'urgence
 - Récupération rapide (article 32, alinéa 1, point c du RGPD) (article 32, alinéa 1, point c du RGPD) ;

4. Procédures de test, d'évaluation et d'évaluation régulières (Article 32 Alinéa 1 Point d du RGPD ; Article 25 Alinéa 1 du RGPD)
 - Gestion de la protection des données ;
 - Gestion des réponses aux incidents ;
 - Protection des données par conception et par défaut (article 25, alinéa 2, du RGPD) ;
 - Contrôle de Commande ou de Contrat
Aucun traitement de données tiers conformément à l'article 28 du RGPD sans instruction correspondante du Client, par exemple : des arrangements contractuels clairs et non ambigus, une gestion des commandes formalisée, des contrôles stricts sur la sélection du prestataire de service, le devoir de pré-évaluation, des contrôles de suivi prudentiels.