Burkhalter Management AG
Hohlstrasse 475, 8048 Zürich
+41 44 432 47 77
www.burkhalter.ch, info@burkhalter.ch

Contrat de traitement des données (CTD) (convention)

entre

Client de la «Déclaration de consentement du contrat de traitement des données»
Responsable du traitement (mandant)

et

Burkhalter Management AG
Hohlstrasse 475, 8048 Zürich en qualité de
Sous-traitant (mandataire)

Le responsable du traitement (partie) et le sous-traitant (partie) forment ensemble les **parties**

concernant

le traitement des commandes selon le droit suisse

1 Objet

(a) Il existe entre les parties un rapport de droit pour l'exécution duquel des données personnelles sont transmises au sous-traitant par le responsable du traitement. La présente convention est conclue entre les parties afin de garantir une protection adéquate lors de la transmission desdites données personnelles. En cas de contradiction entre la présente convention et d'autres contrats, la présente convention prévaut si et dans la mesure où elle est liée au traitement des données personnelles par le mandataire dans le cadre du contrat existant.

1.1 Définitions

(a) Sauf disposition contraire dans la présente convention, tous les termes ont la même signification que dans la loi fédérale sur la protection des données («**LPD**») du 19 juin 1992, resp. du 20 septembre 2020 dès son entrée en vigueur. Toute référence à la LPD doit inclure un renvoi à l'ordonnance actuelle relative à la LPD («**OLPD**») ainsi qu'à toute autre disposition sous-jacente du droit suisse de la protection des données.

(b) En outre, la présente convention aide les parties à se conformer au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 («RGPD UE»). Les renvois au RGPD de l'UE ne sont pertinents que pour les traitements de données auxquels s'applique le RGPD de l'UE. Si des références au RGPD de l'UE donnent naissance à une contradiction avec le droit suisse de la protection des données, ce dernier prévaut.

1.2 Description du traitement des données

(a) Les données personnelles concernées par le présent contrat de traitement ainsi que les finalités du traitement sont décrites dans l'annexe 1 à la présente convention. L'annexe 1 fait partie intégrante de la présente convention et peut être modifiée unilatéralement de temps à autre par le responsable du traitement.

2 Obligations du responsable du traitement

(a) Le responsable du traitement assure

(1) que le transfert des données personnelles et le traitement de ces données par le sous-traitant, tels qu'ils sont décrits dans la présente convention, sont conformes au droit applicable, que le transfert au sous-traitant intervient conformément au droit applicable, et

(2) qu'aucune autre disposition légale n'interdit le transfert du traitement des données.

(b) Le responsable du traitement a acquis la certitude que les mesures techniques et organisationnelles mises en place par le sous-traitant et décrites à l'annexe 2 permettent d'assurer une protection adéquate des données personnelles transférées.

3 Obligations du sous-traitant

3.1 Généralités

(a) En ce qui concerne le traitement des données personnelles selon l'annexe 1, le sous-traitant assure ce qui suit:

(1) Il traitera ces données personnelles conformément à la présente convention et exclusivement aux fins poursuivies par le responsable du traitement.

(2) Les finalités poursuivies par le responsable du traitement ressortent de l'annexe 1 ou des instructions expresses du responsable du traitement ou sont définies par une autre convention avec le responsable du traitement.

(3) Il mettra à la disposition du responsable du traitement les informations nécessaires au contrôle du respect des obligations prévues par la présente convention.

(4) Il respectera les principes de la protection des données dès la conception et par défaut lors de la réalisation de ses outils de travail et de ses produits, applications ou services.

(5) Il informera le responsable du traitement s'il ne peut plus ou prévoit qu'il ne pourra vraisemblablement plus respecter la présente convention.

(6) Il communiquera au responsable du traitement l'adresse de contact pour les demandes relatives à la protection des données et communiquera spontanément les modifications intervenant à cet égard.

(7) Il fournira au responsable du traitement une assistance appropriée dans le cadre des analyses d'impact relatives à la protection des données (selon l'art. 35 RGPD UE) ou des consultations préalables (selon l'art. 36 RGPD UE).

(8) Il coopérera avec les autorités de contrôle compétentes dans les limites admises par la loi.

(b) Les personnes autorisées par le responsable du traitement à donner des instructions sont désignées par écrit au sous-traitant au début du traitement. En cas de changement ou d'absence prolongée de la personne de contact, le sous-traitant doit être informé par écrit et sans délai de l'identité du successeur ou du représentant de la personne de contact. Les instructions orales ne sont contraignantes qu'après confirmation écrite immédiate par le responsable du traitement. Le courrier électronique est réputé constituer une forme écrite suffisante.

(c) Le mandataire doit informer immédiatement le mandant s'il estime qu'une instruction enfreint les dispositions légales. Le mandataire est en droit de suspendre l'exécution de l'instruction en question jusqu'à ce que le responsable du traitement en confirme la licéité ou la modifie.

3.2 Sécurité des données

(a) Pendant la durée de validité de la présente convention, le sous-traitant prend les mesures techniques et organisationnelles appropriées exigées par la LPD et l'art. 32 RGPD UE. Ce faisant, le sous-traitant tient compte de l'état de la technique, des coûts de mise en œuvre ainsi que de la nature, de l'ampleur et des finalités du traitement de même que de la probabilité et de la gravité du risque pour les droits fondamentaux et les droits de la personnalité des personnes concernées. Les mesures sont décrites à l'annexe 2 et sont révisées périodiquement. Des modifications des mesures sont admises dans la mesure où elles ne réduisent pas le niveau de sécurité.

(b) Le sous-traitant

(1) ne fait appel, pour l'exécution des tâches prévues, qu'à des employés tenus à la confidentialité par contrat ou par des dispositions légales et qui ont été préalablement familiarisés avec les dispositions relatives à la protection des données qui les concernent,

(2) informe immédiatement le responsable du traitement et coopère avec lui s'il estime ne plus être en mesure ou risquer de ne plus être en mesure de respecter la présente convention et en particulier les obligations relatives à la sécurité des données,

(3) déploie des mesures appropriées pour aider le responsable du traitement à garantir un niveau de protection des données adapté au risque encouru,

(4) signale immédiatement au responsable du traitement une violation de la sécurité des données (y compris l'accès non autorisé à des données personnelles selon l'annexe 1) et la décrit afin que le responsable du traitement puisse la notifier dans les 72 heures à une autorité de contrôle (selon l'art. 33 RGPD UE) ou aux personnes concernées (selon l'art. 34 RGPD UE). La notification contient au moins i) le type de violation de la sécurité des données, ii) les conséquences de la violation (notamment pour les données selon l'annexe 1), iii) les mesures prises et iv) les mesures prévues.

(c) Sur demande légitime, le mandataire met les rapports sur la sécurité des données à la disposition du responsable du traitement. Le responsable est également en droit de vérifier à ses propres frais le respect de la sécurité des données convenue ou de la faire vérifier par un tiers tenu au secret professionnel. Les contrôles doivent être annoncés à temps et convenus avec le mandataire.

3.3 Sous-traitance secondaire

(a) Le sous-traitant ne peut lui-même sous-traiter le traitement des données à un tiers qu'avec l'autorisation préalable du responsable du traitement. Le responsable du traitement ne doit pas refuser son autorisation sans motif légitime. L'acceptation d'un sous-traitant secondaire par le responsable du traitement ne dégage d'aucune manière le sous-traitant direct de sa responsabilité pour le traitement externalisé des données.

(b) Le sous-traitant est tenu de conclure avec les sous-traitants secondaires des contrats garantissant un niveau de protection des données au moins équivalent à celui prévu par la présente convention.

(c) En règle générale, les services accessoires fournis au mandataire sans rapport avec les données du responsable du traitement selon l'annexe 1 ne sont pas considérés comme une forme de sous-traitance (par ex. services de télécommunication, services postaux et de transport, maintenance et services aux utilisateurs ou élimination de supports de données ainsi que toutes autres mesures visant à assurer la confidentialité, la disponibilité, l'intégrité et la résistance du matériel et des logiciels). Le mandataire reste toutefois tenu, pour les services accessoires aussi, de prendre des mesures de contrôle appropriées afin de garantir la protection et la sécurité des données du mandant.

3.4 Communication à l'étranger

(a) Le traitement des données selon l'annexe 1 intervient en principe en Suisse ou dans un État membre

de l'Union européenne ou dans un autre État signataire de l'accord sur l'Espace économique européen. Une délocalisation dans un autre pays tiers n'est admise que si les conditions légales correspondantes sont remplies (art. 6 LPD ou art. 16 s. LPD du 20 septembre 2020; art. 44 ss. RGPD UE).

(b) Si le sous-traitant direct fait appel à des sous-traitants secondaires exerçant dans des pays qui, selon le préposé fédéral à la protection des données et à la transparence, l'annexe à l'OLPD ou la Commission européenne, ne disposent pas d'un niveau de sécurité approprié, le sous-traitant s'assure que la communication est licite du point de vue de la protection des données en prenant des mesures appropriées au transfert de données concerné. Généralement, le sous-traitant direct convient pour cela avec les sous-traitants secondaires de clauses contractuelles types conformes à la décision d'exécution (UE) 2021/914 de la Commission européenne («clauses contractuelles types modernisées»). Le mandataire convient alors du module approprié (en règle générale le module 3) des clauses contractuelles types modernisées et apporte les adaptations suivantes pour le traitement des données soumises au droit suisse de la protection des données:

(1) Les références au RGPD de l'UE doivent devenir des références à la LPD suisse.

(2) Le préposé fédéral à la protection des données et à la transparence est désigné comme autorité de surveillance.

(3) Le for du domicile des personnes concernées résidant en Suisse ne doit pas être exclu.

(4) Jusqu'à l'entrée en vigueur de la LPD du 20 septembre 2020, la notion de «données personnelles» comprend également les données relatives aux personnes morales.

(c) Pour la collaboration existante avec des sous-traitants établis dans des pays ne disposant pas d'un niveau de sécurité approprié, lequel reste fondé sur les clauses contractuelles types adoptées en vertu de la directive 95/46/CE, les clauses contractuelles types modernisées ou une autre garantie appropriée sont convenues jusqu'au 27 décembre 2022.

4 Droits des personnes concernées

(a) Le responsable du traitement doit fournir aux personnes concernées les informations pour lesquelles elles ont un droit à l'information (droit d'accès), à la communication et à la transmission des données, à la rectification, au blocage, à la suppression ou à l'effacement, conformément à la LPD ou au chapitre III du RGPD de l'UE. Dans ce cadre, le sous-traitant

(1) transmet sans délai au responsable du traitement toute demande relative à des données selon l'annexe 1, sans y répondre lui-même.

(2) collabore avec le responsable du traitement et lui fournit l'assistance nécessaire pour qu'il puisse respecter les droits des personnes concernées, conformément à la LPD ou au chapitre III du RGPD de l'UE.

(3) dans les 15 jours ouvrables, répond de manière complète et conforme à la vérité aux demandes du responsable du traitement ou explique pourquoi sa réponse prendra plus de temps. En aucun cas, le retard ne doit empêcher le responsable du traitement de s'acquitter de ses obligations.

5 Durée et fin

(a) Sauf accord écrit contraire, la présente convention prend fin automatiquement lors de la résiliation du contrat principal ou de la révocation de la «déclaration de consentement du contrat de traitement des données». Néanmoins, les dispositions de la présente convention survivent à la résiliation du contrat principal et subsistent aussi longtemps que le mandataire a les données personnelles en sa possession.

(b) Le responsable du traitement est à tout moment en droit de prononcer une résiliation extraordinaire

de la présente convention pour de justes motifs, dans la mesure où le sous-traitant ne remédie pas à la situation dans un délai raisonnable en dépit d'un avertissement. Il y a justes motifs lorsque le mandataire

(1) viole gravement ses obligations au sens de la présente convention,

(2) viole intentionnellement ou par négligence grave des dispositions de la loi suisse sur la protection des données ou du RGPD de l'UE, ou

(3) ne respecte pas les instructions du responsable du traitement.

(c) À la résiliation de la présente convention, quelle qu'en soit la raison, le sous-traitant direct doit

(1) détruire ou effacer irrémédiablement toutes les données personnelles et leurs copies transférées dans le cadre de la présente convention, obtenir des sous-traitants secondaires qu'ils fassent de même et confirmer l'exécution de cette opération au responsable du traitement, ou

(2) selon le choix du responsable du traitement, restituer immédiatement toutes les données personnelles transférées dans le cadre de la présente convention et obtenir des sous-traitants secondaires qu'ils fassent de même.

(d) Si la législation à laquelle est soumis le sous-traitant lui interdit de restituer ou de détruire tout ou partie des données personnelles, le sous-traitant en informe le responsable du traitement, traite ces données personnelles de manière confidentielle et n'en fait aucun usage actif.

6 Divers

6.1 Compléments

(a) Pour être valables, les modifications, compléments ou annulations de dispositions de la présente convention requièrent la forme écrite. Toute modification de la présente obligation doit faire l'objet d'un accord écrit. Les changements d'adresse doivent être communiqués sans délai à l'autre partie de la manière convenue plus haut.

6.2 Registre des activités de traitement

(a) Sauf exception légale, chaque partie est responsable de la tenue d'un registre des activités de traitement de données.

6.3 Frais

(a) Les frais liés à l'exécution de la présente convention et des obligations qu'elle prévoit sont inclus dans la rémunération convenue dans le contrat principal entre les parties.

6.4 Responsabilité

(a) Si le non-respect de la présente convention par le mandataire, intentionnellement ou à la suite de négligence grave, entraîne des dommages pour le responsable du traitement ou des prétentions de tiers contre lui, le mandataire indemnise le responsable du traitement à cet égard.

6.5 Clause de sauvegarde

(a) Si une disposition de la présente convention devient inapplicable ou invalide, elle n'est annulée que dans la mesure de son inapplicabilité ou de son invalidité et, pour le reste, est remplacée par une disposition valide et applicable reflétant le mieux possible le sens juridique et économique de la disposition invalide. Les autres dispositions de la présente convention restent alors valides et en vigueur.

6.6 Interdiction de cession

(a) La cessibilité des droits et obligations découlant de la présente convention doit être évaluée en fonction des règles du contrat principal. En l'absence de règlementation correspondante dans le contrat principal, il est interdit aux parties de céder ou de transférer à des tiers tout ou partie du présent contrat ou des droits et obligations découlant du présent contrat sans le consentement écrit préalable de l'autre partie. Toute cession ou tout transfert effectué sans le consentement écrit préalable de l'autre partie est nul et non avenu.

6.7 Droit applicable

(a) La présente convention est régie par le droit matériel suisse, à l'exclusion des dispositions relatives aux conflits de lois et de la Convention de Vienne sur les contrats de vente internationale de marchandises.

6.8 For

(a) Les tribunaux ordinaires du siège du responsable du traitement sont seuls compétents pour tout litige découlant de la présente convention ou en rapport avec celle-ci.

Burkhalter Management AG
Hohlstrasse 475, 8048 Zürich
+41 44 432 47 77
www.burkhalter.ch, info@burkhalter.ch

Annexe 1

Finalité du traitement	La finalité du traitement des données personnelles par le sous-traitant réside dans la fourniture au responsable du traitement des services de maintenance et d'assistance décrits dans le contrat principal.
Durée du traitement	Les données personnelles ne sont traitées que pendant la durée du contrat principal ou la durée prévue par la «Déclaration de consentement du contrat de traitement des données»
Catégories de personnes concernées	Membres du personnel, clients, partenaires.
Catégories de données personnelles	Nom, adresse électronique, numéro de téléphone, adresse, date de naissance, profession ou autres informations ou déclarations se référant à une personne déterminée ou pouvant être identifiée au moyen des informations.
Lieu de stockage et de traitement	À l'adresse professionnelle du responsable du traitement et de ses sous-traitants agréés.
Contrôles sur place	Non.
Sous-traitants chargés du traitement	Sous-traitants agréés pour la fourniture des services de maintenance et d'assistance au responsable du traitement décrits dans le contrat principal.
Transfert hors de l'UE/EEE Suisse	Non admis.
Instructions spécifiques ou autres dispositions particulières	Aucunes autres.

Burkhalter Management AG
Hohlstrasse 475, 8048 Zürich
+41 44 432 47 77
www.burkhalter.ch, info@burkhalter.ch

Annexe 2: Mesures techniques et organisationnelles

Description des mesures de sécurité techniques et organisationnelles déployées par le(s) sous-traitant(s):

1 Mesures de sécurité organisationnelles

1.1 Gestion de la sécurité

(a) Politique et procédure de sécurité: le sous-traitant dispose d'une politique de sécurité documentée pour le traitement de données personnelles.

(b) Rôles et responsabilités:

(1) Les rôles et les responsabilités liés au traitement des données personnelles sont clairement définis et attribués conformément à la politique de sécurité.

(2) La révocation des droits et des responsabilités est clairement définie, avec les procédures de transfert correspondantes, en cas de restructuration interne ou de licenciement et de changement de poste.

(c) Politique de contrôle d'accès: des droits de contrôle d'accès spécifiques sont attribués à chaque rôle impliqué dans le traitement des données personnelles, selon le principe du «besoin d'en connaître» (need-to-know).

(d) Gestion des ressources/actifs: le sous-traitant dispose d'un registre des ressources informatiques (matériel, logiciels et réseau) utilisées pour le traitement de données personnelles. Une personne est chargée de la gestion et de la mise à jour du registre.

(e) Gestion des changements: le sous-traitant s'assure que les modifications apportées au système informatique sont enregistrées et surveillées par une personne responsable (par ex. le responsable informatique ou le responsable de la sécurité). Ce processus fait l'objet d'un suivi régulier.

1.2 Réaction aux incidents et continuité des activités

(a) Gestion des incidents ou des violations de la protection des données personnelles:

(1) Un plan de réponse est établi, décrivant les procédures détaillées à mettre en œuvre en cas d'incidents, afin de garantir une réponse efficace et appropriée aux incidents impliquant des données à caractère personnel.

(2) Le sous-traitant notifie sans délai au responsable du traitement tout incident de sécurité ayant entraîné une perte, une utilisation abusive ou une prise de connaissance non autorisée de ses données personnelles.

(b) Continuité des activités: le sous-traitant définit les principales procédures à suivre et les contrôles à effectuer pour assurer le niveau requis de continuité et de disponibilité du système informatique de traitement des données personnelles (en cas d'incident ou de violation de la protection des données personnelles).

1.3 Ressources humaines

(a) Confidentialité du personnel: le sous-traitant s'assure que tous les membres de son personnel connaissent leurs responsabilités et leurs obligations en matière de traitement des données personnelles. Les rôles et les responsabilités en la matière sont clairement communiqués au cours de la procédure préalable à l'embauche et/ou de la formation initiale.

(b) Instruction: le sous-traitant s'assure que tous les membres de son personnel sont bien informés des contrôles de sécurité du système informatique liés à leur travail quotidien. Les membres du personnel impliqués dans le traitement de données personnelles sont en outre informés de manière adéquate, par le biais de campagnes de sensibilisation régulières, des exigences pertinentes en matière de

protection des données et des obligations légales.

2 Mesures de sécurité techniques

2.1 Contrôles d'accès et authentification

(a) Un système de contrôle d'accès a été mis en place et s'applique à l'ensemble des utilisateurs qui accèdent au système informatique. Ce système permet de créer, d'approuver de vérifier et de supprimer des comptes d'utilisateur.

(b) L'utilisation de comptes d'utilisateur par plusieurs personnes est évitée. Lorsque cela est nécessaire, tous les utilisateurs du compte commun doivent avoir les mêmes rôles et responsabilités.

(c) Le principe du «besoin d'en connaître» doit être respecté lors de l'octroi de l'accès ou de l'attribution de rôles aux utilisateurs, afin de limiter le nombre d'utilisateurs ayant accès aux données à caractère personnel aux personnes qui ont besoin de cet accès pour atteindre les finalités du traitement effectué par le sous-traitant.

(d) Si les mécanismes d'authentification sont basés sur des mots de passe, le sous-traitant exige que le mot de passe comporte au moins huit signes et réponde à des critères de contrôle très stricts, notamment la longueur, la complexité des signes et la non-répétabilité.

(e) Les données d'authentification (par ex. identifiant et mot de passe) ne doivent jamais être transmises sur le réseau sans protection.

(f) Il doit être impossible au sous-traitant de gérer les données d'authentification et les contrôles d'accès aux systèmes du responsable du traitement.

2.2 Journalisation et surveillance

(a) Des fichiers journaux sont activés pour l'ensemble des systèmes et applications servant au traitement de données personnelles. Ces fichiers couvrent tous les types d'accès aux données (consultation, modification, suppression).

(b) Le responsable du traitement assure une journalisation des authentifications/accès.

2.3 Sécurité des données en état de veille

(a) Sécurité du serveur et de la base de données

(1) Les serveurs de bases de données et d'applications sont configurés pour utiliser un compte séparé disposant du minimum possible de privilèges sur le système d'exploitation afin de fonctionner correctement.

(2) Les serveurs de bases de données et d'applications ne traitent que les données personnelles dont le traitement est indispensable pour atteindre la finalité convenue.

(3) La sécurité des serveurs et des bases de données de production est assurée par le responsable du traitement et échappe au contrôle du sous-traitant.

(b) Sécurité du poste de travail

(1) Les utilisateurs ne peuvent pas désactiver ou contourner les paramètres de sécurité.

(2) Les applications antivirus et les signatures de détection sont régulièrement mises à jour.

(3) Les utilisateurs n'ont pas le droit d'installer ou de désactiver des applications.

(4) Le système comporte des délais d'expiration au terme desquels une session est automatiquement terminée si l'utilisateur n'a pas été actif pendant un certain temps.

(5) Les mises à jour de sécurité critiques publiées par le développeur du système d'exploitation

sont installées régulièrement.

2.4 Sécurité du réseau et des communications

(a) Lors de chaque accès à Internet, la communication est chiffrée par des protocoles cryptographiques.

(b) Le trafic vers et depuis le système informatique est surveillé et contrôlé par des pares-feux et des systèmes de détection d'intrusion.

2.5 Sauvegardes

(a) Des procédures de sauvegarde et de récupération des données sont définies, documentées et clairement associées aux rôles et aux responsabilités.

(b) Une protection physique et environnementale appropriée est assurée pour les sauvegardes, conformément aux normes applicables aux données d'origine.

(c) L'exécution complète des sauvegardes fait l'objet d'une surveillance.

(d) La stratégie de sauvegarde des systèmes est déterminée par le responsable du traitement et échappe à tout contrôle par le sous-traitant.

2.6 Appareils mobiles/portables

(a) Des procédures sont établies et documentées pour la gestion des appareils mobiles et portables, avec des règles claires pour leur utilisation correcte.

(b) Les appareils mobiles autorisés à accéder au système informatique sont préalablement enregistrés et autorisés.

(c) Le responsable du traitement assure la gestion et l'authentification/l'accès via des appareils mobiles.

2.7 Sécurité pendant le cycle de vie des applications

Les meilleures pratiques, l'état actuel de la technique et des procédures ou normes de développement sûres et reconnues sont respectés tout au long du cycle de développement.

2.8 Effacement/élimination des données

(a) Les données des supports de données sont écrasées par un logiciel avant l'élimination des supports. Lorsque cela n'est pas possible (CD, DVD, etc.), les supports sont physiquement détruits.

(b) Le papier et les supports de données portables comportant des données personnelles sont détruits.

2.9 Sécurité physique

(a) L'environnement physique de l'infrastructure informatique doit être inaccessible pour le personnel non autorisé. Les zones de sécurité et leurs accès doivent être protégés contre l'intrusion de personnes non autorisées par des mesures techniques appropriées (par ex. système de détection d'intrusion, portail à tourniquet commandé par carte RFID, système d'accès sécurisé, système de fermeture) ou des mesures organisationnelles (par ex. service de surveillance).

(b) La sécurité physique de l'infrastructure informatique est assurée par le responsable du traitement et échappe à tout contrôle par le sous-traitant.