Annexe aux conditions générales de vente CASAONE et produits web

Accord sur le traitement des données de commande (ATD) / Data Protection Agreement (DPA)

entre

le client mentionné dans le contrat principal (**Responsable**)

et

Casasoft AG **(Sous-traitant)**
Thurgauerstrasse 36
CH-8050 Zürich

(ensemble: les **Parties**)

1. Objet du contrat

(a) Le Sous-traitant traite les données personnelles pour le compte du Responsable afin de fournir les prestations (**services)** convenues dans le contrat concernant CASAONE et/ou les produits web **(contrat principal).** Ce traitement de données fait l'objet du présent Accord de traitement des données de commande (**ATD**). La version allemande de ce document fait office de version officielle.

(b) Les Parties stipulent que, pour les données de compte principales (généralement les données des collaborateurs et collaboratrices du Responsable à des fins de connexion et de gestion des utilisateurs de l'agent immobilier/l'agence), les deux Parties agissent en tant que contrôleurs distincts. Dans ce cas, elles s'assurent du soutien suffisant de l'autre partie afin de respecter les éventuelles obligations de la loi suisse sur la protection des données. Ces données ne font pas partie du présent Accord sur le traitement des données de commande (ATD).

(c) Objet, nature et finalité: l'objet du traitement des données, sa nature et sa finalité découlent du contrat principal. Le Sous-traitant peut utiliser les données exclusivement sous forme anonyme pour des statistiques, des améliorations de produits et des études de marché.

(d) Cercle des personnes concernées: chasseurs de biens immobiliers et personnes intéressées par des biens immobiliers que l'entreprise du Responsable a publiés à une date actuelle ou antérieure, acheteurs et locataires de ces mêmes biens, utilisateurs internes de l'application CRM CASAONE et ou des produits web tels que les agents immobiliers et autres collaborateurs de l'entreprise du Responsable, personnes entretenant une relation commerciale avec le Responsable ainsi que d'autres tiers, internautes visitant le site web de l'entreprise du Responsable.

(e) Catégories de données personnelles: informations des **personnes à la recherche d'un bien immobilier**, telles que la civilité, le nom, le prénom, l'adresse, les numéros de téléphone, les adresses e-mail, ainsi que d'autres données collectées de manière facultative par le Responsable, comme la date de naissance, la nationalité, le revenu, les éventuels extraits du registre des poursuites, les déclarations d'impôts, les extraits bancaires ou d'autres informations sur la solvabilité, les informations sur l'employeur ou d'autres références, les copies de passeports ou de cartes d'identité, la situation familiale, les préférences d'achat ou de location;
destinataires et expéditeurs, contenus des **e-mails** ou autres messages adressés au Responsable ou émanant de celui-ci;
autres données relatives aux personnes qui entretiennent une **relation commerciale (avec clientèle)** avec le donneur d'ordre, comme les photographes mandatés des biens immobiliers ou d'**autres tiers,** comme les occupants des biens immobiliers en vue d'une visite, etc.; données de base des **donneurs d'ordre du Responsable,** comme leurs personnes de contact, y

compris la raison sociale, le titre du poste, la civilité, le nom, le prénom, l'adresse, les numéros de téléphone, les adresses e-mail, etc.;
autres données telles que celles générées lors de l'**utilisation de services en ligne**, comme les pages web créées pour les biens immobiliers/projets, telles que les données d'accès, les adresses IP, les informations sur les appareils, les fichiers journaux, etc.
Les données citées constituent des exemples types de données collectées dans le cadre de l'activité quotidienne d'agent immobilier du Responsable lors de l'utilisation du logiciel. Les données personnelles spécifiquement concernées découlent des services respectifs et/ou de l'utilisation par le Responsable.

2. Définitions

Les termes suivants ont les significations suivantes:

(a) **Lois sur la protection des données**: (1) la loi fédérale suisse sur la protection des données du 19 juin 1992 (RS 235.1) et l'ordonnance afférente (RS 235.11) ou, à partir du 1er septembre 2023, la loi fédérale suisse révisée sur la protection des données et l'ordonnance afférente (ensemble, la loi suisse sur la protection des données; LPD), (2) le règlement 2016/679 du Parlement européen et du Conseil du 27 novembre 2016 portant sur la protection des personnes physiques lors du traitement des données personnelles, la libre circulation des données et l'abrogation de la directive 95/46/CE (règlement général sur la protection des données; RGPD), et (3) les lois et dispositions relatives à la protection des données d'un État membre de l'UE ou d'un autre pays, dans leur version en vigueur et dans la mesure où elles s'appliquent au traitement des données de commande par le Responsable du traitement et/ou le Sous-traitant;

(b) **Données de commande**: les données personnelles traitées pour le compte du Responsable par ou pour le Sous-traitant dans le cadre du contrat principal;

(c) **Sous-traitant ultérieur**: toute personne (à l'exception d'un collaborateur du Sous-traitant ou d'un de ses sous-traitants ultérieurs) chargée par le Sous-traitant ou en son nom de traiter des données de commande en rapport avec le contrat principal. Ne sont pas considérés comme des sous-traitants ultérieurs les fournisseurs de prestations annexes, dans la mesure où il n'y a pas d'accès systématique aux données de commande (par exemple, les fournisseurs de maintenance et d'assistance, les fournisseurs de

télécommunications et de services postaux). Dans de tels cas, l'obligation du Sous-traitant de garantir des mesures de sécurité adéquates conformément au point 5 du présent ATD demeure réservée et doit être transférée par le Sous-traitant aux fournisseurs de prestations annexes.

(d) Les termes **Responsable, personne concernée, État membre, données personnelles** (et/ou données à caractère personnel), **violation de la protection des données personnelles, traitement** (et/ou manipulation) et **autorités de surveillance** ont les significations attribuées à ces termes dans les lois sur la protection des données.

(e) Sauf définition différente figurant dans le présent ATD, les définitions du contrat principal sont appliquées.

3. Position du Responsable

Le Responsable garantit la fiabilité de la collecte, du traitement et de l'utilisation des données de commande, dont l'instauration de la transparence nécessaire et le respect des droits légaux des personnes concernées (comme l'accès, la rectification ou l'effacement) de manière démontrable.

4. Obligations du Sous-traitant

(a) Respect des instructions:

(i) Le Responsable donne instruction au Sous-traitant de ne traiter les données qu'en conformité avec le contrat principal (y compris le présent ATD) et le droit applicable: (a) pour fournir, sécuriser et surveiller les services et les services d'assistance technique (TSS); et (b) comme (i) l'utilisation des services et des TSS par le Responsable et (ii) toute autre instruction écrite donnée par le Responsable et acceptée par le Sous-traitant en tant qu'instruction dans le cadre du présent ATD (abrégées ci-après en «Instructions»). Le Sous-traitant informera immédiatement le Responsable si, selon l'avis du Sous-traitant: (a) le droit applicable interdit au Sous-traitant de se conformer à une Instruction; (b) une Instruction n'est pas conforme à la législation applicable en matière de protection des données; ou (c) le Sous-traitant n'est pas en mesure de se conformer à une Instruction pour une autre

raison, à moins qu'une telle notification ne soit interdite par le droit applicable.

(ii) Dans la mesure où le Sous-traitant peut interagir directement avec les données de commande dans le cadre des services (par exemple via une interface technique avec les systèmes du Responsable), les Instructions doivent en principe être données de cette manière. Les autres Instructions doivent être données sous forme de texte (c'est-à-dire par écrit, par fax ou par e-mail), sous réserve d'Instructions orales suivies d'une confirmation sous forme de texte en cas d'urgence.

(b) Confidentialité: le Sous-traitant s'engage à traiter les données de commande de manière confidentielle et à ne les rendre accessibles qu'aux personnes ayant besoin d'y avoir accès pour remplir leurs obligations. Il s'assure que toutes les personnes ayant accès aux données de commande sont soumises à une obligation de confidentialité légale ou contractuelle.

(c) Obligation de suppression et de restitution:

(i) Si le Responsable souhaite conserver les données de commande à la fin de la durée du contrat, il peut ordonner au Sous-traitant, pendant la durée du contrat, de restituer les données de commande ainsi que tous les supports de données éventuellement remis. Sinon, les données de commande doivent être définitivement supprimées ou, si cela n'est pas possible, anonymisées, conformément aux Instructions du Responsable et sous réserve d'obligations légales contraires.

(ii) Le Sous-traitant et les sous-traitants ultérieurs sont autorisés à stocker les données de commande dans des systèmes d'archivage et de sauvegarde non utilisés en production, conformément à leurs procédures habituelles et appropriées.

5. Sécurité des données

(a) Mesures de sécurité: le Sous-traitant prend les mesures techniques et organisationnelles décrites en Annexe 2 pour protéger les données de commande (**mesures de sécurité**) et les maintient pendant toute la durée du contrat. Le Responsable a vérifié les mesures de sécurité et les juge adéquates et suffisantes. Le Sous-traitant est autorisé à adapter les mesures de sécurité,

à condition que le niveau de sécurité ne soit pas abaissé. Les adaptations doivent être documentées.

(b) Communication des violations: en cas de violation de la protection des données de commande, le Sous-traitant informe le Responsable dans les meilleurs délais et dans tous les cas en fournissant les informations requises par la loi (ces informations pouvant être transmises de manière échelonnée si elles ne sont pas connues immédiatement).

6. Sous-traitants ultérieurs

(a) Conditions préalables: pour la fourniture des services, le Sous-traitant peut transmettre des données de commande à des sous-traitants ultérieurs. En cas de recours à un sous-traitant ultérieur, le Sous-traitant veillera, par le biais d'un contrat écrit, à ce que le sous-traitant ultérieur n'accède aux données de commande et ne les utilise que dans l'étendue nécessaire à l'exécution des obligations qui lui incombent, et ce conformément au présent ATD.

(b) Sous-traitants ultérieurs à l'étranger: dans la mesure où des données de commande en rapport avec le recours à un sous-traitant ultérieur parviennent dans un pays n'offrant pas un niveau de protection des données suffisant et/ou sont accessibles depuis ce pays, et dans la mesure où le donneur d'ordre n'a pas convenu de garanties correspondantes avec le Sous-traitant, le Sous-traitant est tenu et autorisé par le Responsable à prévoir, avant la première communication de données du Responsable au sous-traitant ultérieur concerné, des garanties appropriées conformément à la législation sur la protection des données (en particulier les clauses contractuelles types de l'UE) et à les maintenir pendant toute la durée du contrat.

(c) Approbation: une liste des sous-traitants ultérieurs existants ayant accès aux données de commande figure en Annexe 1. Avant toute modification des relations de sous-traitance, le Responsable en sera informé par écrit. Si, dans un délai de deux semaines, il ne déclare pas expressément et par écrit qu'il n'est pas d'accord avec la modification pour des raisons importantes, la modification en question sera considérée comme acceptée. Si le Responsable s'oppose à la modification par écrit dans les deux semaines suivant la réception de la communication susmentionnée, les Parties chercheront de bonne foi une alternative acceptable pour les deux Parties. Si les Parties ne parviennent pas à se mettre d'accord sur une alternative dans un délai d'un

mois à compter de la notification de l'opposition, chaque partie a le droit de résilier tous les services concernés sans frais. Dans ce cas, le Sous-traitant est tenu de procéder conformément au point (c) quant aux données de commande concernées.

(d) Responsabilité: le Sous-traitant doit répondre du respect des obligations des sous-traitants ultérieurs à l'égard du Responsable.

7. Droits de contrôle

(a) Droit de contrôle: le Responsable a le droit de vérifier, à ses propres frais, le respect par le Sous-traitant des obligations légales et contractuelles en rapport avec le traitement des données de commande du présent ATD. Les contrôles doivent être effectués après notification écrite au moins 20 jours ouvrables à l'avance, pendant les heures de bureau habituelles et sans perturber de manière déraisonnable les activités du Sous-traitant. Les Parties conviennent au préalable de la date, de la durée et de l'objet des contrôles ainsi que des dispositions applicables en matière de sécurité et de confidentialité.

(b) Fréquence: le Responsable ne procède pas à des contrôles plus d'une fois par année civile. Il se réserve toutefois le droit de procéder à d'autres contrôles dans des cas justifiés – notamment en cas d'indices d'un traitement de données de commande contraire au contrat ou aux instructions ou encore d'une augmentation imprévue et importante des risques.

(c) Confidentialité: le Responsable traite de manière confidentielle les informations fournies par le Sous-traitant dans le cadre d'un tel contrôle.

(d) Organisme de contrôle externe: le Sous-traitant a le droit de faire réaliser l'audit à ses propres frais par un organisme externe compétent et tenu à la confidentialité. Le Sous-traitant met le rapport d'audit à la disposition du Responsable.

8. Coopération

(a) Respect des obligations légales en matière de protection des données: le Sous-traitant assiste le Responsable comme il se doit dans le respect des obligations légales en matière de protection des données.

(b) Droits des personnes concernées: dans la mesure où une personne concernée s'adresse au Sous-traitant concernant des exigences légales en matière de protection des données, le Sous-traitant transmet immédiatement la demande au Responsable.

(c) Droit d'information: les actions de contrôle et autres mesures prises par les autorités de surveillance de la protection des données doivent être communiquées au Responsable dans les meilleurs délais si elles concernent les données de commande ou les systèmes utilisés pour leur traitement.

(d) Remboursement des frais: le Sous-traitant peut facturer sans supplément les dépenses occasionnées par les actions de soutien prévues au présent point 8, dans la mesure où une obligation correspondante ne découle pas déjà du contrat principal. Il ne dispose cependant pas d'un droit de refus de prestation.

(e) Contact: pour les questions portant sur la protection des données, les personnes suivantes doivent être contactées:

Responsable: mes personnes de contact du Responsable figurant dans le contrat principal doivent être contactées.
Sous-traitant: support@casasoft.ch

9. Responsabilité

La responsabilité des Parties est soumise aux dispositions du contrat principal.

10. Durée et fin

(a) Le présent ATD entre en vigueur à sa signature ou, si le contrat principal est conclu ultérieurement, à la signature du contrat principal, et prend fin à la résiliation du contrat principal.

(b) Le Responsable est en droit de résilier le présent ATD sans préavis pour motif grave si le Sous-traitant enfreint gravement les dispositions du présent ATD, s'il ne peut ou ne veut pas exécuter une instruction du Responsable conforme au contrat ou s'il refuse les droits de contrôle du Responsable en violation du contrat.

11. Ordre de priorité des contrats

Sauf stipulation contraire du présent Accord, les dispositions du contrat principal s'appliquent.

12. Clauses finales

(a) Le Responsable est en droit d'adapter le contrat principal et/ou le présent ATC par notification écrite au moins 30 jours à l'avance, dans la mesure où cela est nécessaire pour respecter les lois sur la protection des données ou une injonction contraignante d'une autorité. Les Parties se proposent de négocier en temps utile des adaptations du présent ATC, dans la mesure où une adaptation de l'ATC selon la phrase précédente représente une charge excessive pour le Sous-traitant.

(b) Dans la mesure où la rémunération convenue dans le contrat principal ne couvre pas déjà les obligations de coopération et d'assistance du Sous-traitant conformément au présent ATC, le Sous-traitant a droit au remboursement des frais justifiés, concrètement occasionnés. Le point 8(d) s'applique.

1 Annexe 1: Sous-traitants ultérieurs

Informations concernant le lieu		Informations concernant le traitement des données
Adresse	Pays	Finalité du traitement de données
SMG Swiss Marketplace Group, Werdstrasse 21, 8048 Zürich, Suisse	Suisse	Hébergement du système de fichiers CASAONE (par exemple, PDF et images des biens immobiliers)
Holycode, Jurija Gagarina 12, Beograd, Serbie	Serbie	Développement de logiciels, maintenance en tant qu'extension de notre équipe de développeurs suisses
Modis Contracting Solutions GmbH, Friedrichstraße 6, 70174 Stuttgart, Allemagne	Allemagne	Développement de logiciels, maintenance avec des experts temporaires de notre équipe de développeurs suisses
DigitalOcean, 101 6th Ave, New York, NY 10013, États-Unis	États-Unis (lieu du serveur Francfort)	Hébergement CASAGATEWAY (pour la publication d'annonces immobilières sur des portails)
Amazon Web Services, Mythenquai 10, 8002 Zürich, Suisse	Suisse (lieu du serveur Zurich)	Hébergement du logiciel CASAONE CRM, crypté
WP Engine 504 Lavaca St #1000, Austin, TX 78701, États-Unis	États-Unis (lieux du serveur Belgique et Pays-Bas)	Hébergement de divers sites web immobiliers et de sites web de projets faisant partie des produits web de CASASOFT.
Infomaniak, Infomaniak Network SA, Rue Eugène Marziano 25, 1227 Les Acacias, Suisse	Suisse	Sauvegardes pour nos produits au cas où les fournisseurs susmentionnés ne seraient plus disponibles
Mandrill Mailchimp, The Rocket Science Group, LLC 675 Ponce de Leon Ave NE Suite 5000, Atlanta, GA 30308, États-Unis	États-Unis	Envoi d'e-mails transactionnels tels que des notifications par e-mail lorsque de nouveaux messages sont disponibles

ActiveCampaign, 1 North Dearborn St 5th Floor Chicago, IL 60602, États-Unis	États-Unis	Envoi d'e-mails marketing sur les produits de CASASOFT à nos clients
Aircall, 381 Park Avenue South, 16th Floor, New York, NY 10016, États-Unis	États-Unis	Notre équipe d'assistance répond aux appels des collaborateurs et collaboratrices à l'aide de ce logiciel
Atlassian, Atlassian. Pty Ltd, Level 6, 341 George Street, Sydney NSW 2000, Australie	Australie (centre de données dans la région Europe)	Notre équipe d'assistance traite les tickets d'assistance et les e-mails entrants au moyen de ce logiciel.
Datadog, 620 8th Ave 45th Floor New York, NY 10018, États-Unis	États-Unis	Stockage des fichiers journaux du système, surveillance et analyse du système
New Relic, 188 Spear Street, Suite 1000, San Francisco, CA 94105, États-Unis	États-Unis	Surveillance, débogage et analyse des performances du système
Sentry, Functional Software, Inc., 45 Fremont Street, 8th Floor, San Francisco, CA 94105, États-Unis	États-Unis	Stockage des fichiers journaux du système, surveillance et analyse du système

2 Annexe 2: Mesures de sécurité

Ci-joint l'aperçu des mesures de sécurité actuelles du Sous-traitant. Les mesures de sécurité sont contrôlées en permanence par des audits.

Les mesures techniques et organisationnelles peuvent être adaptées en permanence et sans adaptation du contrat par le fournisseur, à condition que le niveau de sécurité existant ne baisse pas.

Les éventuelles autres mesures de sécurité sont définies dans le contrat principal (et/ou dans ses annexes).

Contrôle d'accès physique

1) Définition des zones de sécurité

2) Réalisation d'une protection d'accès physique efficace

3) Définition des personnes disposant de droits d'accès physiques

4) Gestion et documentation des droits d'accès personnels tout au long du cycle de vie

5) Accompagnement des visiteurs et du personnel externe

6) Surveillance des locaux en dehors des heures de bureau

7) Enregistrement de l'accès physique

Contrôle d'accès au système

1) Protection de l'accès au système (authentification)

2) Authentification simple des collaborateurs et collaboratrices (au moyen d'un nom d'utilisateur et d'un mot de passe) avec application d'un niveau de sécurité élevé

3) Blocage de l'accès en cas d'échec ou d'inactivité et processus de réinitialisation des accès bloqués

4) Interdiction de stocker des mots de passe ou des entrées de formulaire en dehors de la solution interne de gestion des mots de passe

5) Définition des personnes autorisées

6) Administration et documentation des supports d'authentification personnels et des autorisations d'accès

7) Blocage automatique de l'accès au système

8) Blocage manuel de l'accès au système

9) Transmission sécurisée des données d'authentification / d'accès sur le réseau

10) Enregistrement des accès au système

Contrôle d'accès aux données

1) Création d'un concept d'autorisation

2) Mise en œuvre de restrictions d'accès aux données

3) Attribution standard des droits d'accès minimum nécessaires

4) Administration et documentation de l'autorisation pour l'accès personnel aux données

5) Enregistrement des accès aux données

Contrôle du transport / de la transmission

1) Sécurisation de la transmission des données entre le serveur et le client

2) Sécurisation de la transmission des données dans les systèmes backend

3) Sécurisation de la transmission des données vers les systèmes externes

4) Implémentation de passerelles de sécurité sur les nœuds de transmission du réseau

5) Durcissement des systèmes backend

6) Description de toutes les interfaces et des champs de données personnelles transmises

7) Authentification machine-machine

8) Gestion des supports de données (procédure)

9) Processus de collecte et de destruction des supports de données

10) Procédure d'effacement et de destruction axée sur la protection de la vie privée

Contrôle des saisies

1) Documentation des personnes autorisées à effectuer des saisies

2) Journalisation des entrées

Contrôle de la disponibilité

1) Concept de sauvegarde

2) Gestion de la continuité des activités / Plan d'urgence

3) Stockage de sauvegarde

4) Inspection et test de l'infrastructure de secours

Règles de séparation des fonctions

1) Collecte minimisée et efficace des données

2) Traitement séparé des données

Autres standards de développement liées à la sécurité

1) Principe du double contrôle

2) Scan de sécurité des applications et des référentiels, scan du pipeline CI/CD