Contrat de traitement des données par un tiers entre

Client

– ci-après dénommé le responsable –

et

optovision GmbH
Heinrich-Hertz-Str. 17
63225 Langen

– ci-après dénommé le sous-traitant des données –

Cet accord de traitement par un tiers (AVV) règle le traitement des données personnelles du responsable et définit les droits et obligations concernant les aspects de la protection des données - sur la base de la nouvelle loi fédérale suisse sur la protection des données (LPD révisée) et du règlement général de l'Union européenne sur la protection des données (RGPD-UE).

§ 1 Objet et durée du mandat

(1) Le sous-traitant des données exécute les services décrits à l'annexe 1 pour le compte du responsable du traitement. L'objet, la nature et la finalité du traitement, le type de données et les catégories de personnes concernées y sont décrits.

(2) Sauf dispositions contraires, le présent contrat entre en vigueur à la signature des deux parties et reste valable tant que le sous-traitant des données traite des données personnelles pour le compte du responsable du traitement. Il prend fin automatiquement à la fin de la relation commerciale ou à la fin du contrat principal.

§ 2 Instructions du responsable du traitement

(1) Le responsable du traitement est chargé de veiller au respect des dispositions légales en matière de protection des données, notamment à la licéité du traitement ainsi qu'au respect des droits des personnes concernées. Les dispositions légales ou contractuelles en matière de responsabilité n'en sont pas affectées.

(2) Le sous-traitant des données traite les données personnelles mises à sa disposition exclusivement selon les instructions du responsable du traitement et dans le cadre des accords conclus. Les données ne peuvent être rectifiées, effacées et bloquées que si le responsable du traitement en donne l'instruction.

(3) Le traitement n'est effectué que sur instruction du responsable du traitement, à moins que le sous-traitant des données ne soit tenu de traiter ces données en vertu du droit de l'Union européenne ou des États membres auquel le sous-traitant des données est soumis. Dans ce cas, le sous-traitant des données communique ces exigences légales au responsable du traitement avant le traitement, à moins que le droit en question n'interdise cette communication pour un motif d'intérêt public important.

(4) En principe, les instructions peuvent être données oralement. Les instructions orales doivent ensuite être documentées par le responsable du traitement. Les instructions doivent être données par écrit ou sous forme de texte si le responsable du traitement le demande.

(5) Si le sous-traitant des données estime qu'une instruction donnée par le responsable du traitement est contraire à la législation sur la protection des données, il doit en informer immédiatement le responsable du traitement.

§ 3 Mesures techniques et organisationnelles

(1) Le sous-traitant des données s'engage à prendre des mesures de sécurité techniques et organisationnelles appropriées pour les données à traiter et à les documenter dans l'annexe 3 du présent contrat. Les mesures de sécurité doivent garantir un niveau de protection adapté au risque.

(2) Les mesures prises peuvent être adaptées au fil du temps en fonction des évolutions techniques et organisationnelles. Le sous-traitant des données ne peut procéder à de telles adaptations que si celles-ci atteignent au moins le niveau de sécurité des mesures antérieures. Sauf disposition contraire, le sous-traitant des données ne doit communiquer au responsable du traitement que les adaptations importantes.

(3) Le sous-traitant des données assiste le responsable du traitement dans le respect de toutes les obligations légales relatives aux mesures techniques et organisationnelles à respecter. Le sous-traitant des données doit, sur demande, contribuer à l'établissement et à la mise à jour du registre des activités de traitement du responsable du traitement. Le sous-traitant des données participe à l'élaboration d'une analyse d'impact relative à la protection des données et, le cas échéant, à la consultation préalable des autorités de surveillance. Il doit communiquer au responsable du traitement, sur demande, toutes les informations et tous les documents nécessaires.

§ 4 Obligations du sous-traitant des données

(1) Le sous-traitant des données confirme qu'il connaît les dispositions légales applicables en matière de protection des données. Il conçoit, dans son domaine de responsabilité, l'organisation interne de l'entreprise de manière à satisfaire aux exigences particulières de la protection des données.

(2) Le sous-traitant des données fournit des garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles appropriées pour assurer que le traitement est conforme à la législation sur la protection des données et aux droits de la personne concernée.

(3) Le sous-traitant des données garantit qu'il familiarise les collaborateurs employés pour l'exécution des travaux avec les dispositions relatives à la protection des données qui leur sont applicables et que les personnes autorisées à traiter les données à caractère personnel sont tenues à la confidentialité ou sont soumises à une obligation légale appropriée de garder le secret. Il veille au respect des dispositions légales relatives à la protection des données.

(4) Dans le cadre du traitement des données par un tiers, le sous-traitant des données ne peut accéder aux données personnelles du responsable du traitement que si cela est absolument nécessaire à l'exécution du traitement.

(5) Le traitement des données par un tiers est en principe effectué en Suisse, dans l'Espace économique européen (EEE) ou dans d'autres États dont la législation en matière de protection des données garantit, selon l'appréciation du Préposé fédéral à la protection des données et à la transparence (PFPDT) ou du Conseil fédéral suisse, une protection adéquate des données. Toute délocalisation dans d'autres États ne peut se faire qu'avec l'accord du responsable du traitement et aux conditions de la loi fédérale sur la protection des données (LPD) et dans le respect du présent contrat.

(6) Le sous-traitant des données assiste le responsable du traitement en prenant les mesures techniques et organisationnelles appropriées afin que le responsable du traitement puisse remplir ses obligations existantes envers la personne concernée, telles que l'information et le renseignement de la personne concernée, la rectification ou l'effacement des données, la limitation du traitement ou le droit à la portabilité des données et à l'opposition au traitement. Le sous-traitant des données désigne un interlocuteur qui assiste le responsable du traitement dans l'exécution des obligations légales d'information et de renseignement qui surviennent dans le cadre du traitement des données par un tiers et communique immédiatement ses coordonnées au responsable du traitement. Dans la mesure où le responsable du traitement est soumis à des obligations légales particulières d'information en cas de prise de connaissance illicite de données, le sous-traitant des données assiste le responsable du traitement à cet égard. Le sous-traitant des données ne peut fournir des informations à la personne concernée ou à des tiers que sur instruction préalable du responsable du traitement. Dans la mesure où une personne concernée fait valoir ses droits en matière de protection des données directement auprès du sous-traitant des données, ce dernier transmettra immédiatement cette demande au responsable du traitement.

§ 5 Autorisation d'établir des relations de sous-traitance

(1) Le sous-traitant des données ne peut faire lui-même appel à des sous-traitants que si le responsable du traitement le lui a préalablement autorisé par écrit.

(2) Il y a notamment relation de sous-traitance lorsque le sous-traitant des données confie à d'autres sous-traitants des données, en partie ou en totalité, des prestations auxquelles se rapporte le présent contrat. Ne sont pas considérées comme des relations de sous-traitance au

sens de la présente réglementation les services que le sous-traitant des données sollicite auprès de tiers en tant que prestation accessoire pour l'aider dans l'exécution de son mandat. Il s'agit par exemple de services de télécommunication ou de personnel de nettoyage. Le sous-traitant des données est toutefois tenu, afin de garantir au responsable du traitement la protection et la sécurité des données de conclure des accords contractuels appropriés et conformes à la loi, même pour les prestations accessoires sous-traitées et de prendre des mesures de contrôle.

(3) L'accès aux données par le sous-traitant du sous-traitant des données ne peut avoir lieu que si le sous-traitant des données garantit, par un contrat écrit, que les dispositions convenues dans ce contrat s'appliquent également à son sous-traitant, des garanties suffisantes devant notamment être fournies pour que les mesures techniques et organisationnelles appropriées soient mises en œuvre de manière à ce que le traitement soit effectué conformément aux dispositions de la législation sur la protection des données.

(4) Le recours aux sous-traitants énumérés à l'annexe 2 au moment de la signature du contrat est réputé approuvé, pour autant que les conditions mentionnées à l'article 5, paragraphe 3, du présent contrat soient mises en œuvre.

§ 6 Droits de contrôle du responsable du traitement

Le sous-traitant des données accepte que le responsable du traitement ou une personne mandatée par ses soins soit autorisé(e) à contrôler le respect des dispositions relatives à la protection des données et des accords contractuels dans la mesure nécessaire, notamment en demandant des informations et documents pertinents, en consultant les programmes de traitement ou en accédant aux locaux de travail du sous-traitant des données pendant les heures de bureau indiquées, après notification préalable. Des certificats appropriés et valables en matière de sécurité informatique (par ex. protection informatique de base, ISO 27001) peuvent également apporter la preuve d'un traitement conforme, dans la mesure où l'objet de la certification s'applique également au traitement des données par un tiers dans le cas concret. La présentation d'un certificat pertinent ne remplace toutefois pas l'obligation du sous-traitant des données de documenter les mesures de sécurité au sens de l'article 3 du présent accord.

§ 7 Violations à notifier du sous-traitant des données

Le sous-traitant des données informe immédiatement le responsable du traitement de toute perturbation du fonctionnement de l'entreprise entraînant des risques pour les données du responsable du traitement, ainsi qu'en cas de suspicion de violation de la protection des données en rapport avec les données du responsable du traitement. Il en va de même si le sous-traitant des données constate que les mesures de sécurité qu'il a prises ne répondent pas aux exigences légales. Le sous-traitant des données sait que le responsable du traitement est tenu de documenter de manière exhaustive toutes les violations de la protection des données personnelles et, le cas échéant, de les signaler immédiatement aux autorités de contrôle ou à la personne concernée. Si de telles violations ont eu lieu, le sous-traitant des données aidera le responsable du traitement à respecter ses obligations de notification. Il signalera sans délai les violations commises par le responsable du traitement et communiquera au moins les informations suivantes :

a) une description du type de violation, des catégories et du nombre approximatif de personnes et d'enregistrements de données concernés,

b) le nom et les coordonnées d'une personne à contacter pour de plus amples informations,

c) une description des conséquences probables de la violation et

d) une description des mesures prises pour remédier à la violation ou l'atténuer.

§ 8 Fin du mandat

(1) Au terme traitement des données par un tiers, le sous-traitant des données doit, au choix du responsable du traitement, soit effacer toutes les données personnelles, soit les restituer, à moins qu'il n'existe une obligation légale de conserver les données personnelles.

(2) Le responsable du traitement peut résilier la relation contractuelle sans préavis si le sous-traitant des données commet une violation grave des dispositions du présent contrat ou des dispositions relatives à la protection des données et si, en raison de cette violation, la poursuite du traitement des données jusqu'à l'expiration du délai de préavis ou jusqu'à la fin convenue du mandat ne peut être raisonnablement exigée.

§ 9 Dispositions finales

(1) Si la propriété du responsable du traitement chez le sous-traitant des données est menacée par des mesures prises par des tiers (par exemple par une saisie ou une confiscation), par une procédure d'insolvabilité ou par d'autres événements, le sous-traitant des données doit en informer immédiatement le responsable du traitement. Un droit de rétention est exclu en ce qui concerne les supports de données et les stocks de données du responsable du traitement.

(2) La conclusion du contrat, ses modifications et clauses accessoires doivent être rédigées par écrit, ce qui, à partir du 25.05.2018, peut également être fait dans un format électronique.

(3) Si certaines parties du présent contrat sont invalides, cela n'affecte pas la validité du reste du contrat.

Annexe 1 : Liste des services mandatés et coordonnées des préposés à la protection des données

Objet du traitement	• L'accord s'applique à toutes les prestations pour lesquelles le responsable du traitement transmet, pendant la durée de l'exécution mandat, des données personnelles à des sous-traitants des données qui sont nécessaires à l'exécution du mandat en question. Il couvre toutes les activités en rapport avec le mandat sous-jacent et au cours desquelles les collaborateurs du sous-traitant des données ou les tiers mandatés par ce dernier peuvent entrer en contact avec des données personnelles du responsable du traitement.
Nature et finalité du traitement	• La nature et la finalité du traitement des données personnelles par le sous-traitant des données pour le compte du responsable du traitement sont toutes les prestations de services que Rodenstock fournit au client. Ces services peuvent comprendre, entre autres, les activités et objectifs suivants : - Collecte et traitement de données à caractère personnel transmises dans le cadre du traitement de commandes de verres de lunettes et de produits optiques. - L'installation, la mise à disposition et le suivi (service sur site et télémaintenance) des équipements tels que les scanners Vision Excellence Tower 4.0, etc. - Mise à disposition d'un service client (notamment la télémaintenance) - Mise à disposition et prestation de services publicitaires
Type de données à caractère personnel	• Données du responsable du traitement (utilisateur), par ex. titre, nom, prénom, société, adresse postale, adresse e-mail, numéros de téléphone et de fax, date de naissance, données médicales, fonction • Données clients du responsable du traitement, par ex. titre, nom, prénom, sexe, adresse postale, adresse e-mail, numéro de téléphone, données médicales (y compris les photographies du fond de l'œil, les évaluations des analyses, les commentaires)
Catégories de personnes concernées	• Le client et son personnel • Les clients du responsable du traitement

Nom et coordonnées du préposé à la protection des données du responsable du traitement (s'il est connu)	
Nom et coordonnées du préposé à la protection des données du sous-traitant des données	optovision GmbH z.Hd. Datenschutzbeauftragter (À l'attention du délégué à la protection des données) Heinrich-Hertz-Str. 17 63225 Langen E-Mail: datenschutz@optovision.com

Annexe 2 : Liste des sous-traitants des données mandatés, y compris les sites du traitement

Sous-traitants des données mandatés (nom, forme juridique, siège de la société)	**Site du traitement**	**Type de prestation de service**
WACON Internet GmbH	Nollenweg 2, D-65510 Idstein / Germany	Administration du site Internet de l'entreprise
CLDES	Sonnenberger Str. 52B, D-65193 Wiesbaden / Germany	Création et production de mailings

Annexe 3: Mesures techniques et organisationnelles en vue de garantir la sécurité du traitement des données

Cette annexe documente les mesures techniques et organisationnelles mises en œuvre par le sous-traitant des données pour la bonne exécution du service fourni.

Les contractants sont tenus de mettre en œuvre les mesures techniques et organisationnelles appropriées de manière à ce que le traitement des données soit effectué conformément aux exigences légales et que la protection des droits de la personne concernée soit assurée de manière adéquate.

Mesures	**Mise en œuvre de la mesure**
A. Mesures de pseudonymisation Il s'agit de mesures visant à limiter les références immédiates aux personnes dans le cadre du traitement des données, de sorte que l'identification d'une personne en particulier soit uniquement possible si les données sont combinées avec d'autres informations. Des mesures techniques et organisationnelles appropriées doivent être mises en place afin de conserver ces informations complémentaires séparément du pseudonyme.	• Pseudonymisation des données personnelles dans le cadre des études de marché
B. Mesures de chiffrement Il s'agit de mesures ou processus consistant à utiliser un procédé de codage (système de chiffrement) pour rendre illisible un texte ou une information clairs et intelligibles, les convertissant en une suite de caractères difficiles à interpréter	• Chiffrement de client VPN TLS> 1.1 • Chiffrement de VPN site à site AES256, 3DES • Les sites Web utilisant l'authentification utilisateur sont chiffrés à l'aide du protocole TLS • Stockage chiffré des mots de passe au sein du système central
C. Mesures de garantie de la confidentialité **1. Contrôle des accès** Il s'agit de mesures visant à empêcher les personnes non autorisées d'accéder physiquement aux systèmes informatiques et installations utilisés pour le traitement des données personnelles, ainsi qu'aux dossiers et supports de données confidentiels	• Les ordinateurs sont verrouillés lorsque les personnes quittent le poste de travail. • Porte sécurisée (système d'entrée électronique, etc.) • Salle de serveurs sécurisée • Accès au site : barrière • Accès aux bâtiments : carte à puce, lecteur de badges, contrôle lors de la remise des clés • Accès à la salle de serveurs : carte à puce est réservée à certains collaborateurs • Accès aux sauvegardes de données est réservé aux personnes autorisées (périmètre restreint) • Dispositifs de surveillance vidéo sur le site

2. Contrôle des accès Il s'agit de mesures visant à empêcher l'exploitation ou le traitement de données protégées par des personnes non autorisées	• Chiffrement des chemins d'accès : SSL ou AES256 • Service d'annuaire (Active Directory) • Mise à jour régulière des filtres antivirus et anti-logiciels espions • Système de droits d'accès : nombre limité de collaborateurs autorisés • Pare-feu • L`accès Wi-Fi des invités est en dehors du réseau de l'entreprise. • Collaborateurs / appareils Wi-Fi protégés par une clé de sécurité personnelle (PSK) • Installation d'antivirus au moment de la mise en service des ordinateurs et mise à jour régulière
3. Contrôle des accès Il s'agit de mesures visant à garantir que les personnes autorisées à effectuer des opérations de traitement des données peuvent accéder uniquement aux données sur lesquelles elles bénéficient d'une autorisation. L'objectif est que les données ne puissent pas être consultées, copiées, modifiées ou supprimées par des personnes non autorisées lors de leur traitement ou de leur utilisation, ou lorsqu'elles sont stockées	• Les interfaces utilisateurs et les modifications de rôles sont demandées service par service. La vérification est à la charge du responsable du centre de coûts, la mise en œuvre dépendant quant à elle des administrateurs informatiques • Serveur Active Directory : l'octroi des droits est centralisé au niveau de chaque site et assuré par le personnel du service informatique • La consigne est donnée à tous les collaborateurs de vérifier l'absence de logiciels malveillants sur les clés USB avant de les utiliser. • L'accès aux sauvegardes de données est réservé aux personnes autorisées (périmètre restreint)
4. Impératif de séparation Il s'agit de mesures visant à garantir que les données recueillies à différentes fins sont traitées à part et conservées séparément des autres données et systèmes, de façon à empêcher toute utilisation de ces données à des fins autres que celles prévues	• Rôles spécifiques aux différentes activités pour l'accès aux fichiers • Systèmes individuels (PGI/serveurs de fichiers/bases de données) installés chacun sur des systèmes distincts • Séparation entre les systèmes utilisés pour les tests et pour la production • Autorisations
D. Mesures de garantie de l'intégrité **1. Intégrité des données** Il s'agit de mesures visant à garantir que les données personnelles stockées ne seront pas endommagées en cas de dysfonctionnement du système	• Test de fonctionnement lors de l'installation, puis correctifs et mises à jour par le service informatique • L'installation des versions (Releases) et des correctifs (Patches) se fait dans le progiciel de gestion intégré (PGI) avec le système de tickets Redmine. Il y a toujours d'abord une installation dans les systèmes de test. La gestion des correctifs clients et serveurs sur les systèmes Microsoft est effectuée à l'aide de Matrix-42. • Les correctifs base de données sont appliqués de manière cyclique par les

	administrateurs sur la base des messages des fabricants. Le déploiement sur les systèmes de test a toujours lieu en premier. Des tests sont effectués avant une installation opérationnelle. Caractéristiques particulières de l'instruction de procédure : • Documentation Les exigences, les risques, les spécifications de test, les résultats de test, l'architecture, les installations et les mises à jour sont documentés par écrit et de manière à ce qu'ils puissent être révisés. • Processus Processus et responsabilités définis pour les tâches de nouveau développement et de maintenance. • Risque Toutes les fonctionnalités concernant l'intégrité des données doivent être soumises à une procédure de test ; en fonction du risque concernant l'intégrité des données, des mesures sont prises pour les garantir.
2. Contrôle des échanges Il s'agit de mesures visant à garantir la vérifiabilité et le contrôle des emplacements de destination des données personnelles lors de la transmission ou de la mise à disposition de ces données, au moyen d'installations spécifiques	• Identification • Autorisations utilisateur spécifiques à chaque système
3. Contrôle des transports Il s'agit de mesures visant à garantir que la confidentialité et l'intégrité des données personnelles sont préservées lors de leur transmission et lors du transport des supports de données	• Tunnel VPN entre les sociétés du groupe (MPLS) • Accès aux sauvegardes de données est réservé aux personnes autorisées (périmètre restreint) • Principe de responsabilité individuelle pour les procédés de transport • Procédés de chiffrement permettant de détecter toute modification des données au cours de leur transport
4. Contrôle de saisie Il s'agit de mesures visant à garantir la vérifiabilité et le contrôle des opérations de saisie, modification ou suppression effectuées sur les données personnelles au niveau des systèmes utilisés pour leur traitement.	• Consignation des modifications et archivage des journaux ainsi créés (système PGI)

E. Mesures de garantie de la disponibilité et de la fiabilité **1. Contrôle de la disponibilité** Il s'agit de mesures visant à garantir la protection des données personnelles contre la destruction accidentelle ou la perte	• Les principaux serveurs sont dédoublés. Cela concerne également les systèmes de disques RAID matériels. • Les principaux systèmes sont répartis dans deux centres de données distincts. • Alimentations sans interruption dédoublées avec sous-distribution également dédoublée dans les deux centres de données. • Installations électriques de secours dans les deux centres de données. • Systèmes de détection d'incendie dans les deux centres de données. • Systèmes de climatisation dédoublés dans chaque centre de données. • Systèmes virtuels avec VMWare • Protection spéciale pour l'accès aux centres de données, aux bandes et aux chambres fortes. • Surveillance des systèmes critiques • Centre de calcul IBM séparé en 2 sites de centre de calcul.
2. Récupération rapide Il s'agit de mesures visant à garantir notre capacité à restaurer la disponibilité des données personnelles et l'accès à celles-ci en cas d'incident technique ou d'accident.	• Plan de secours avec manuel pour les situations d'urgence • Procédures de sauvegarde des données • Tests périodiques de récupération des données avec construction de nouveaux systèmes de test • Systèmes virtuels avec VMWare • Réseau de stockage SAN d'IBM dédoublé (Stretched Cluster)
3. Fiabilité du système Il s'agit de mesures visant à garantir que toutes les fonctions du système sont opérationnelles et que les dysfonctionnements sont dûment signalés	• Surveillance automatique avec notifications e-mail • Plans de secours avec désignation de personnes responsables • Disponibilité d'un service informatique d'urgence
F. Mesures relatives à la réalisation d'évaluations périodiques de la sécurité du traitement des données **1. Procédures de contrôle** Il s'agit de mesures visant à garantir un traitement des données à la fois sécurisé et conforme aux prescriptions en vigueur	• Gestion de la protection des données • Procédés formalisés en cas d'incident compromettant la protection des données • Vérification annuelle des systèmes informatiques par des auditeurs externes • Délégué à la protection des données • Signalement des incidents relatifs à la protection des données au délégué à la protection des données, à la direction du service informatique et à la direction générale • Maintenance régulière des installations techniques/contrats de maintenance • Tests de fonctionnement des groupes diesel de secours

2. Contrôle de la bonne exécution du Contrat Il s'agit de mesures visant à garantir que les données personnelles exploitées dans le cadre de l'exécution du Contrat peuvent être traitées dans le plus strict respect des instructions du Client.	• Documentation des instructions du Client (voir l'accord sur l'exécution des missions)