ACCORD DE SOUS-TRAITANCE (ACCORD ST)

entre

Client / Société
Personne responsable du traitement
Adresse postale

- dans ce qui suit : Mandant

et

Idiligo B.V.
Kabelweg 57
NL-1014 Amsterdam

- dans ce qui suit : Sous-traitant

le contrat suivant est conclu :

§ 1 Préambule

Les parties contractantes planifient ou entretiennent déjà une relation d'affaires. Le présent accord concrétise les obligations des parties contractantes sur la protection des données, qui découlent du contrat sous-jacent (ci-après dénommé « Contrat ») : « Contrat principal ») dans leurs détails. L'activité décrite dans le contrat susmentionné constitue un traitement de données de commande. Il est donc nécessaire que les parties contractantes concluent un accord sur le traitement des données de commande, conformément à l'article 28 du Règlement général sur la protection des données (RGPD) de l'UE.
Cet accord s'applique à toutes les activités qui sont liées au contrat principal et dans le cadre desquelles les employés du Sous-traitant ou les personnes mandatées par celui-ci traitent les données à caractère personnel du Mandant.

§ 2 Responsabilité

(1) Dans le cadre de ce contrat, le Mandant est responsable du respect des dispositions légales, notamment de la licéité du traitement des données (« Responsable du traitement» au sens de l'art. 4 chiffre 7 du RGPD).
(2) Aux fins du traitement, le Sous-traitant tient lui-même un répertoire des traitements qu'il effectue au sens de l'article 30 du RGPD. Sur demande, il fournira au Mandant les informations nécessaires à la vue d'ensemble conformément à l'art. 30 du RGPD.
(3) Dans la mesure où le Sous-traitant, en violation de la présente convention et du RGPD, détermine lui-même les finalités et les moyens du traitement, il est considéré comme responsable de ce traitement aux sens de l'art. 4 chiffre 7 du RGPD.

§ 3 Définitions

(1) « Sous-traitant » : toute personne physique ou morale, autorité publique, agence ou autre organisme qui traite des données à caractère personnel pour le compte du Responsable du traitement

(2) « Données à caractère personnel » : toute information concernant une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée »)

(3) « Traitement » : toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, le classement, la conservation (stockage), l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que la limitation, l'effacement ou la destruction

(4) « Instruction » est l'ordre du Mandant à un certain traitement de protection des données (par exemple, anonymisation, blocage, suppression, publication) du Sous-traitant avec des données à caractère personnel.

(5) « Sous-traitant du Sous-traitant » : tout autre sous-traitant du Sous-traitant au sens de l'art. 28, al. 4, du RGPD

(6) « Tiers » : toute personne physique ou morale, autorité publique, agence ou tout autre organisme, autre que la personne concernée, le responsable du traitement, le Sous-traitant et les personnes qui, sous l'autorité directe du responsable du traitement ou du Sous-traitant, sont autorisées à traiter les données à caractère personnel

(7) « Pays tiers » : un pays situé en dehors de l'Union européenne et de l'Espace économique européen

§ 4 Objet et durée du contrat/du traitement

(1) L'objet de la commande est dérivé du contrat principal auquel il est fait référence ici.

(2) Dans la mesure où l'objet ne résulte pas ou pas complètement du contrat principal, l'objet du traitement est le suivant : Idiligo B.V. accorde au Mandant une licence non transférable et non exclusive pour l'utilisation de l'application Idiligo, conformément aux dispositions des « Conditions générales, 3. Licence et utilisation » d'Idiligo B.V., en détail

   a) Idiligo donne accès à l'application Idiligo (connexion de l'utilisateur via le site web d'Idiligo B.V.)

   b) L'application Idiligo permet au Mandant de créer ses propres utilisateurs pour son compte Idiligo

   c) Le Mandant peut développer et utiliser des scripts de manière indépendante. Grâce à ces scripts, il peut, par exemple, documenter aussi des informations spécifiques au Mandant.

   d) Le Mandant a accès à ses informations documentées.

(3) La durée de la commande est fonction de la durée du contrat principal, sauf disposition contraire dans les dispositions du présent accord.
(4) Le droit de résiliation sans préavis pour motif valable reste inchangé.

§ 5 Portée, nature et finalité du traitement ainsi que type de données à caractère personnel et catégories de personnes concernées

(1) Dans la mesure où la portée, le type et la finalité du traitement ne sont pas déjà spécifiés dans le contrat principal, les dispositions suivantes s'appliquent en complément.
(2) En particulier, les données suivantes font partie du traitement des données

Nature des données	**Catégories de personnes concernées par le Mandant**
Données de base de la personne	Clients
Coordonnées (e-mail, téléphone)	Employés
Données sur les clients	Parties intéressées
Données de communication (streaming audio et vidéo, partage d'écran)	Candidats
Données de contenu (fichiers partagés dans des scripts, chat textuel, contenu de tableau blanc)	Fournisseurs
Journaux d'activité (fichiers journaux)	Abonnés
Données de signature (caractéristiques de la signature numérique)	Contractant
Données contractuelles (documents juridiques sous-jacents avec signature numérique)	Représentant commercial / partenaire
Données du calendrier (date, durée)	Travailleurs indépendants
	Interlocuteur du Mandant
Données des tickets d'assistance (messages et historiques de chat entre les utilisateurs et le contractant dans le cadre des demandes d'assistance)	
Métadonnées (statistiques d'utilisation) • Journaux d'activité (fichiers journaux) • Adresse IP • Cookies • Trafic API • Contrôle/Signalisation du trafic • Fichiers journaux du serveur de médias • Fichiers journaux d'accès à la plate-forme	

§ 6 Pouvoir de donner des instructions

(1) Le traitement des données à caractère personnel par le Sous-traitant est effectué exclusivement dans le cadre des accords conclus et conformément aux instructions documentées du Mandant, sauf dans un cas exceptionnel au sens de l'art. 28 al. 3a du RGPD.
Pour autant que le Mandant le juge nécessaire, les personnes autorisées à donner des instructions peuvent être nommées. Le Mandant doit en informer le contractant par écrit ou sous forme de texte. Si ces personnes habilitées à donner des instructions changent chez le Mandant, le contractant doit en être informé par écrit ou sous forme de texte de la ou des nouvelles personnes nommée(s) à cet égard.

(2) Les instructions sont initialement énoncées dans le contrat principal et peuvent ensuite être modifiées, complétées ou remplacées par des instructions individuelles écrites ou sous forme électronique (format texte) par le Mandant à l'organisme désigné par le Sous-traitant (instruction individuelle). Les instructions qui ne sont pas prévues dans le contrat principal sont traitées comme une demande de modification des prestations.

(3) Les instructions orales doivent être confirmées immédiatement par écrit ou sous forme de texte.

(4) Le Sous-traitant doit informer le Mandant sans délai s'il considère qu'une instruction viole des lois applicables. Le Sous-traitant peut suspendre l'exécution de l'instruction jusqu'à ce qu'elle ait été confirmée ou modifiée par le Mandant.

(5) Le Sous-traitant veille à ce que les employés participant au traitement des données du Mandant et les autres personnes travaillant pour le Sous-traitant s'interdisent de traiter les données en dehors du champ d'application de la mission.

(6) Les modifications de l'objet du traitement et les changements de procédure sont couverts par le pouvoir du Mandant de donner des instructions et doivent être documentés en conséquence. En cas de modification de la commande que le Sous-traitant considère comme substantielle, le Sous-traitant a le droit de s'y opposer. Si le Mandant insiste sur la modification malgré l'objection du Sous-traitant, cette modification sera considérée comme un motif valable et permettra la résiliation sans préavis de l'accord ST affecté par l'instruction ainsi que des éléments de l'accord principal correspondant affectés par l'accord ST.

Les modifications de l'objet du traitement et les changements de procédure sont couverts par le pouvoir du Mandant de donner des instructions et doivent être documentés en conséquence. En cas de modification substantielle de la commande, le Sous-traitant a le droit de s'y opposer. Si le Mandant insiste sur la modification malgré l'objection du Sous-traitant, cette modification sera considérée comme un motif valable et permettra la résiliation sans préavis de l'accord ST affecté par l'instruction ainsi que des éléments de l'accord principal correspondant affectés par l'accord ST.

§ 7 Lieu d'exécution/transfert vers un pays tiers

Le Sous-traitant fournira les services contractuels dans l'Union européenne (UE) ou dans l'Espace économique européen (EEE) ou dans un pays tiers. Tout sous-traitant du Sous-traitant fournira les services qui le concernent dans l'Union européenne (UE) ou dans l'Espace économique européen (EEE) ou dans un pays tiers. Si un service est fourni par le Sous-traitant ou le sous-traitant du Sous-traitant dans un pays tiers, le titulaire doit garantir le respect des dispositions pertinentes du RGPD et en apporter la preuve à la demande du Mandant.

(1) Dans la mesure où le traitement des données peut être effectué en dehors de l'Allemagne conformément au présent accord et aux exigences légales pour le traitement des données personnelles pour le compte de tiers ou pour le transfert de données personnelles à l'étranger, le Sous-traitant veillera au respect et à la mise en œuvre des exigences légales afin de garantir un niveau de protection des données adéquat en cas de déménagement et de trafic de données transfrontalier.

§ 8 Protection du secret / de la confidentialité des données et des secrets d'affaires

(1) Le Sous-traitant s'assure que les personnes autorisées à traiter les données à caractère personnel se soient engagées à respecter la confidentialité ou soient soumises à une obligation légale de secret convenable. L'obligation de confidentialité/secret continue à s'appliquer après l'exécution de la commande.

(2) En outre, le Sous-traitant est tenu de traiter de manière confidentielle toute connaissance des secrets d'affaires et des mesures de sécurité des données du Mandant acquise dans le cadre de la relation contractuelle.

(3) En outre, toutes les personnes du Sous-traitant sont tenues de respecter les obligations de garder les secrets d'affaires du Mandant et doivent être informées du §4 de la Loi pour la protection des secrets d'affaires (GeschGehG).

§ 9 Mesures techniques et organisationnelles

(1) Dans son domaine de responsabilité, le Sous-traitant conçoit l'organisation interne de manière à ce qu'elle réponde aux exigences particulières de la protection des données. Il prend les mesures techniques et organisationnelles nécessaires à la protection appropriée des données personnelles du Mandant, qui suffisent aux exigences du RGPD (art. 28 al. 3 lettre c, 32 du RGPD).

(2) Le Sous-traitant prend les mesures techniques et organisationnelles nécessaires pour assurer la confidentialité, l'intégrité, la disponibilité et la résilience à long terme des systèmes et des services en rapport avec le traitement.

(3) Le Sous-traitant veille à remplir les obligations qui lui incombent en vertu de l'article 32, alinéa 1, lettre d), du RGPD, à savoir mettre en œuvre une procédure de contrôle régulier de l'efficacité des mesures techniques et organisationnelles destinées à assurer la sécurité du traitement.

(4) Quant au respect des mesures de protection convenues, ce qui suit sera considéré comme accordé

- Pour le respect des mesures de protection convenues et de leur efficacité vérifiée, on se réfère aux règles de conduite approuvées conformément à l'art. 40 du RGPD, que le Sous-traitant a présenté le 25 septembre 2020 et dont le respect a été vérifié et confirmé le 6 octobre 2020.

(5) Le Sous-traitant se réserve le droit de modifier les mesures de sécurité prises, à condition de s'assurer que le niveau de protection ne tombe pas en dessous du niveau convenu par contrat.

(6) Le Sous-traitant documente la mise en œuvre des mesures techniques et organisationnelles décrites et requises avant le début du traitement de la commande, en particulier en ce qui concerne l'exécution concrète de la commande, et les remet au Mandant pour son examen et approbation.

(7) Une description des mesures techniques et organisationnelles convenues figure à l'annexe 1 du présent accord.

§ 10 Sous-traitance, autres sous-traitants (sous-traitants du Sous-traitant)

(1) Aux fins de la présente disposition, on entend par relations de sous-traitance les services qui sont directement liés à la fourniture du service dans le cadre du contrat principal. Cela n'inclut pas les services auxiliaires que le Sous-traitant utilise, par exemple comme services de télécommunications, services postaux/transport, maintenance et service aux utilisateurs ou élimination des supports de données ou autres mesures visant à garantir la confidentialité, la disponibilité, l'intégrité et la résilience du matériel et des logiciels des systèmes de traitement des données.

Toutefois, afin de garantir la protection et la sécurité des données du Mandant, le Sous-traitant est tenu de prendre des accords contractuels et des mesures de contrôle appropriés et conformes à la loi pour s'assurer que les données du Mandant soient protégées, même dans le cas de services auxiliaires externalisés.

(2) Le Mandant autorise le Sous-traitant à utiliser les services d'autres Sous-traitants (sous-traitants du Sous-traitant) conformément aux alinéas du § 10 de la présente convention. Cette autorisation constitue une autorisation écrite générale au sens de l'art. 28, al. 2 du RGPD.

(3) La transmission des données à caractère personnel du Mandant au sous-traitant du Sous-traitant et sa première action ne sont autorisées qu'après que toutes les conditions requises pour une sous-traitance aient été remplies.

(4) Si le sous-traitant du Sous-traitant fournit le service convenu en dehors de l'UE/de l'EEE, le Sous-traitant doit assurer la recevabilité au regard de la législation sur la protection des données en prenant les mesures appropriées. Il en va de même lorsqu'il s'agit de recourir à des prestataires de services au sens de l'alinéa 1, deuxième phrase.

(5) Toute externalisation ultérieure par le sous-traitant du Sous-traitant nécessite le consentement exprès du Mandant principal (au moins sous forme de texte) ; toutes les règles contractuelles de la chaîne contractuelle doivent également être imposées au sous-traitant du Sous-traitant ultérieur.

(6) Au moment de la conclusion de cet accord, les entreprises énumérées à l'annexe 3 sont des sous-traitants du Sous-traitant pour des prestations partielles qui travaillent pour le Sous-traitant et qui traitent et/ou utilisent directement les données du Mandant dans ce contexte. Ces sous-traitants du Sous-traitant sont réputés être autorisées à mener les activités dont concernées par le le présent accord.

(7) Le Mandant ne peut s'opposer à l'utilisation d'un sous-traitant du Sous-traitant que pour des raisons valables.

§ 11 Correction, suppression et blocage des données

(1) Pendant la durée de la mission, le Sous-traitant ne peut corriger, supprimer ou bloquer les données contractuelles que selon les instructions du Mandant.

(2) Si une personne concernée doit contacter directement le Sous-traitant pour faire corriger, effacer ou bloquer ses données, le Sous-traitant transmettra immédiatement cette demande au Mandant.

§ 12 Assistance du Sous-traitant en cas d'obligations au titre des articles 12 à 23, 33 à 36 du RGPD

(1) Le Sous-traitant soutient le Mandant dans la mesure de ses possibilités pour répondre aux demandes et aux revendications des personnes concernées conformément aux articles 12 à 23 du RGPD (obligations d'information, droits des personnes concernées, droit d'être oublié, droit à la portabilité des données, etc.)

(2) Le Sous-traitant soutient le Mandant dans l'accomplissement des obligations d'information vis-à-vis de l'autorité de surveillance compétente ou des personnes concernées par une violation de la protection des données à caractère personnel conformément aux articles 33 et 34 du RGPD.

(3) Le Sous-traitant soutient le Mandant dans l'évaluation des incidences sur la protection des données conformément à l'article 35 du RGPD avec toutes les informations dont il dispose. S'il est nécessaire de consulter préalablement l'autorité de surveillance compétente en vertu de l'art. 36 du RGPD, le Sous-traitant assistera également le Mandant à cet égard.

§ 13 Obligations de notification du Sous-traitant

(1) Le Sous-traitant informe immédiatement le Mandant

a) en cas de violation par le Sous-traitant ou les personnes employées par lui dans le cadre de l'exécution de la commande des dispositions relatives à la protection des données à caractère personnel du Mandant ou des dispositions prévues dans le contrat. Il prendra les mesures nécessaires pour sécuriser les données et minimiser les éventuelles conséquences négatives pour les personnes concernées et consultera immédiatement le Mandant à ce sujet ;

b) s'il estime qu'une instruction viole les lois applicables ;

c) sur les actions et les mesures de contrôle prises par les autorités de surveillance, dans la mesure où elles se réfèrent à l'objet du présent accord. Cela s'applique également lorsqu'une autorité compétente enquête, dans le cadre d'une procédure administrative ou pénale, sur le traitement de données à caractère personnel relatives au traitement de commandes chez le Sous-traitant.

(2) Si les données du Mandant sont mises en danger dans les locaux du Sous-traitant par une saisie ou une confiscation, par une procédure d'insolvabilité ou de concordat ou par d'autres événements ou mesures prises par des tiers, le Sous-traitant en informera le Mandant sans délai. Le Sous-traitant informera immédiatement toutes les personnes responsables du traitement dans ce contexte que le Mandant est le seul souverain et propriétaire des données en tant que « responsable du traitement » au sens du règlement général sur la protection des données.

§ 14 Retour et suppression des données et des supports de données à la fin du contrat

(1) À l'issue des prestations de traitement, le Sous-traitant doit soit effacer soit restituer toutes les données à caractère personnel au Mandant, au choix de ce dernier, sauf si, selon le droit de l'Union européenne ou le droit national applicable au Sous-traitant, une obligation de conserver les données à caractère personnel est prescrite. L'enregistrement de la suppression est fourni sur demande

(2) Dans la mesure où le transport du support de stockage avant sa suppression est indispensable, le Sous-traitant prend les mesures appropriées pour le protéger, notamment contre le vol, la lecture, la copie ou la modification non autorisées. Si nécessaire, les mesures et les procédures de suppression à appliquer seront convenues en détail en plus des descriptions de service.

(3) Les documents qui servent de preuve du traitement ordonné et adéquat des données sont conservés par le Sous-traitant conformément aux périodes de conservation respectives au-delà de la fin du contrat. Il peut les remettre au Mandant à la fin du contrat pour le décharger.

(4) Si le Mandant n'est pas en mesure de retirer les données, il en informera le Sous-traitant par écrit en temps utile. Le Sous-traitant est alors autorisé à supprimer les données à caractère personnel au nom du Mandant.

(5) Dans le cas des matériaux d'essai et de rejet, un ordre individuel concernant la suppression n'est pas nécessaire, ceux-ci doivent être supprimés.

§ 15 Droits de contrôle du Mandant et droits d'acquiescement et de participation

(1) Le Sous-traitant fournit au Mandant, par des moyens appropriés, les preuves du respect des obligations prévues dans le présent contrat.

(2) Le Sous-traitant peut apporter des preuves, notamment en fournissant les informations suivantes :

a) Mise en œuvre d'un auto-audit
b) Attestation d'un expert
c) Règles de conduite internes de l'entreprise, y compris les preuves externes de conformité
d) Certificat sur la protection des données et/ou la sécurité de l'information (par exemple ISO 27001)
e) des règles de conduite approuvées conformément à l'article 40 du RGPD
f) Certificats selon l'art. 42 du RGPD

(3) Si l'auditeur mandaté par le Mandant est en relation de concurrence avec le Sous-traitant, ce dernier dispose d'un droit d'opposition à son encontre.

(4) L'exécution du contrôle de la commande au moyen de vérifications régulières par le Mandant en ce qui concerne l'exécution ou la réalisation du contrat, en particulier le respect et, le cas échéant, l'adaptation nécessaire des règlements et des mesures pour l'exécution de la commande, est soutenue par le Sous-traitant. En particulier, le Sous-traitant s'engage à fournir au Mandant, sur demande écrite, qui peut également être sous forme électronique, dans un délai raisonnable, toutes les informations nécessaires à l'exécution d'un contrôle.

(5) Le Mandant doit informer immédiatement et complètement le Sous-traitant s'il découvre des erreurs ou des irrégularités concernant les règles de protection des données lors de la vérification.

§ 16 Nomination d'un délégué à la protection des données

(1) Le Sous-traitant désigne un délégué à la protection des données, pour autant que les exigences de l'article 37 du RGPD soient respectées.

(2) Le Mandant doit être informé immédiatement par écrit ou sous forme de texte d'un changement de délégué à la protection des données. Le Sous-traitant veille à ce que les exigences relatives au délégué à la protection des données et à ses activités conformément à l'article 38 du RGPD soient respectées.

(3) Si aucun délégué à la protection des données n'a été désigné chez le Sous-traitant, celui-ci désigne une personne de contact pour le Mandant.

(4) Si le siège du Sous-traitant est situé en dehors de l'Union européenne, il désigne un représentant dans l'Union conformément à l'article 27, alinéas 1 et 3, alinéa 2, du RGPD.

(5) Les personnes à nommer conformément aux alinéas 1 à 4 sont désignées à l'annexe 2 du présent accord.

§ 17 Responsabilité

(1) Le Mandant et le Sous-traitant sont conjointement et solidairement responsables envers la personne concernée de tout dommage causé par un traitement non conforme au RGPD.

(2) Le Sous-traitant est responsable exclusivement des dommages résultant des traitements effectués par lui dans les cas suivants

a) il n'a pas respecté les obligations résultant du RGPD et spécifiquement imposées aux Sous-traitants, ou

b) il a agi au mépris des instructions légalement données par le Mandant, ou

c) il a agi à l'encontre des instructions légalement données par le Mandant.

(3) Dans la mesure où le Mandant est tenu de payer des dommages et intérêts à la personne concernée, le Mandant se réserve le droit d'avoir recours au Sous-traitant.

(4) Toutefois, dans le cadre de la relation interne entre le Mandant et le Sous-traitant, le Sous-traitant n'est responsable des dommages causés par le traitement que si

a) il n'a pas respecté les obligations qui lui sont spécifiquement imposées par le RGPD, ou

b) il a agi au mépris des instructions légalement données par le Mandant ou contre ces instructions.

(5) Les autres droits à la responsabilité selon les lois générales restent inchangés.

§ 18 Clause de forme écrite

(1) Les modifications et les compléments à la présente annexe et à tous ses éléments - y compris toute assurance donnée par le Sous-traitant - nécessitent un accord écrit, qui peut également être sous forme électronique (format texte), et l'indication expresse qu'il s'agit d'une modification ou d'un complément aux présentes conditions générales. Cela vaut également pour la dispense de cette exigence formelle.

§ 19 Clause de sauvegarde

(1) En cas de contradictions, les dispositions du présent accord sur la protection des données prévalent sur les dispositions du contrat principal.

(2) Si certaines dispositions du présent accord s'avéraient totalement ou partiellement invalides ou inapplicables ou devenaient invalides ou inapplicables à la suite de changements législatifs intervenus après la conclusion de l'accord, les autres dispositions de l'accord et la validité de l'accord dans son ensemble ne seraient pas affectées.

(3) La disposition invalide ou inexécutable est remplacée par une disposition valide et applicable qui se rapproche le plus possible du sens et de l'objectif de la disposition invalide.

(4) Si le contrat s'avère incomplet, les dispositions qui correspondent au sens et à l'objet du contrat et qui auraient été convenues si le contrat avait été considéré sont réputées avoir été convenues.

§ 20 Applicabilité

(1) Le présent accord s'applique dès sa signature par les parties.

(2) À partir du 25 mai 2018, le RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE (règlement général sur la protection des données) s'appliquera.

§ 21 Choix de la loi et du lieu de juridiction

(1) Le droit néerlandais s'applique.

(2) Le lieu de juridiction est le siège social du Sous-traitant.

[Lieu], le [JJ.MM.AAAA]	Amsterdam, le [JJ.MM.AAAA]
[nom complet AG]	Idiligo B.V.
_____	_____
[Mandant]	[Sous-traitant / Contractant]

Annexes :

Annexe 1 : Mesures techniques et organisationnelles

Annexe 2 : Nomination du délégué à la protection des données, de la personne de contact et/ou du représentant au sein de l'Union européenne

Annexe 3 : Sous-traitants du Sous-traitant utilisés

Annexe 4 : Lieux de service convenus conformément au § 7

Annexe 1

Mesures technico-organisationnelles

1. Confidentialité (article 32, alinéa 1, lettres a) et b), du RGPD)

Contrôle d'accès

L'accès non autorisé doit être empêché, le terme devant être compris dans le sens d'un espace.
Mesures techniques et organisationnelles pour le contrôle d'accès, en particulier pour la légitimation des personnes autorisées :

☒ Détermination des personnes autorisées, y compris l'étendue des pouvoirs respectifs
☒ Sélection minutieuse du personnel de nettoyage
☒ Délivrance de badges d'autorisation d'accès
☒ Existence d'une réglementation pour les personnes extérieures (accompagnement du visiteur par des employés,
Séparation des zones de traitement et d'audience)
☒ Mise en œuvre d'un règlement clé
☒ Enregistrement des personnes entrantes et sortantes

Mesures physiques en place et régulièrement contrôlées :

☒ Entrée sécurisée (par exemple, portes verrouillables, serrures de sécurité)
☒ Sécurité des portes (ouvre-porte électrique)
☒ Fenêtres anti-effraction
☒ Protection des appareils contre le vol, la manipulation ou les dommages
☒ Matériel de surveillance (par exemple, un système d'alarme, une vidéosurveillance)
☒ Système de séparation (par exemple, tourniquet, écluse)
☒ Personnel de sécurité, portiers
☒ Subdivision en différentes zones de sécurité

Divers :

Contrôle d'accès

Il faut empêcher l'intrusion de personnes non autorisées dans les systèmes de traitement des données et l'utilisation non autorisée du système.

Mesures techniques et organisationnelles concernant l'identification et l'authentification des utilisateurs :

- ☒ Conception et mise en œuvre d'un concept d'autorisation
- ☒ Concept d'autorisation pour les dispositifs terminaux (ordinateurs)
- ☒ Concept d'autorisation pour les logiciels/systèmes
- ☒ Identification et vérification de l'autorisation d'un utilisateur
- ☒ Mise en place d'un système de gestion des identités des utilisateurs
- ☐ Suivi des tentatives d'accès avec réaction aux incidents de sécurité
- ☒ Définition et contrôle des droits d'accès
- ☒ Procédure d'authentification en fonction du besoin de protection des informations (classification)
- ☒ Cryptage
- ☐ Verrouillage des interfaces externes (USB, etc.)
- ☒ Protection appropriée par mot de passe (règles de conduite, archives cryptées)
- ☒ Logiciels de sécurité spéciaux (anti-malware, scanner de virus, pare-feu logiciel et matériel)
- ☒ Authentification à deux facteurs
- ☒ Existence d'une réglementation pour les entreprises externes
- ☒ Fonction d'accès par jeton

Divers :

Contrôle d'accès

Il faut empêcher les activités non autorisées dans les systèmes de traitement des données en dehors du champ d'application de l'autorisation accordée.

La conception du concept d'autorisation et des droits d'accès, ainsi que leur surveillance et leur enregistrement sur la base de :

- ☒ Concept d'autorisation et de rôles pour les applications
- ☒ Mise en œuvre de la réglementation pour l'autorisation de l'accès et aux utilisateurs
- ☒ Vérification des autorisations
- ☒ Limitation des fonctions (fonctionnelle/temporelle)
- ☒ Restrictions d'accès (selon le « Need-to-Know » et « Least Privilege » (« besoin de savoir » et « moindre privilège »))
- ☒ Stockage de données cryptées
- ☒ Journalisation des accès aux applications, notamment lors de la saisie, de la modification et de la suppression des données
- ☒ Enregistrement des tentatives d'accès non autorisées
- ☐ Évaluation régulière
- ☒ Évaluation liée à l'événement
- ☒ Mise en œuvre de la réglementation relative à la suppression des données
- ☒ Mise en œuvre de la réglementation relative à l'élimination des supports de stockage (utilisation de destructeurs de documents ou bien de prestataires de services conformément à la norme DIN 66933)
- ☒ Mise en œuvre de la réglementation relative à la manipulation des supports de stockage électroniques
- ☒ Contrôle de l'intégrité

Divers :

Contrôle de la séparation

Les données collectées pour différentes finalités sont traitées séparément.

Les mesures de traitement séparé (stockage, modification, suppression, transmission) de données ayant des finalités différentes :

Capacité multi-mandants :

- ☒ Séparation physique
- ☒ Séparation logique des mandants (côté logiciel)
- ☒ Séparation de la production et des systèmes d'essai
- ☒ Sandboxing (Bac à sable)
- ☒ Définition des droits sur les bases de données
- ☐ Documentation de la séparation des fonctions (n'est pas applicable)
- ☒ Existence de lignes directrices et d'instructions de travail
- ☒ Existence de documents de procédure
- ☒ Contrôle régulier de l'utilisation prévue des informations et les systèmes informatiques

Divers :

Pseudonymisation et cryptage

Le traitement de données à caractère personnel de telle sorte que les données ne puissent plus être attribuées à une personne concernée spécifique sans informations complémentaires, à condition que ces informations complémentaires soient conservées séparément et fassent l'objet de mesures techniques et organisationnelles appropriées :

- ☒ Trusted Third Party (Tiers de confiance)
- ☐ Signature aveugle
- ☒ Cryptage logiciel pour le stockage des données
- ☐ Cryptage matériel pour le stockage des données

Divers :

2. Intégrité (art. 32, alinéa 1, lettre b), du RGPD)

Contrôle de la divulgation

Les aspects relatifs à la divulgation et au transfert de données à caractère personnel devraient être réglementés : Transmission électronique, transport de données, contrôle de la transmission. Les mesures relatives au transport, à la transmission et à la communication ou au stockage sur des supports de données (manuels ou électroniques) et à la vérification ultérieure :

Pour les supports de données électroniques :

- ☒ Cryptage de la transmission de données (par exemple, VPN, S/MIME)
- ☒ Signature électronique
- ☒ Mise en œuvre de protocoles de transfert ou de transmission de données
- ☒ Réalisation de contrôles de plausibilité, d'exhaustivité et d'exactitude selon les besoins
- ☒ Mesures visant à empêcher le flux incontrôlé d'informations (par exemple, désactivation des interfaces USB, contrôles réguliers des destinataires autorisés, restriction technique aux destinataires autorisés)
- ☒ Documentation des formes de transfert de données (par exemple, impression, supports de données, transmission automatisée)
- ☒ Transmission de données sous forme anonyme ou avec pseudonyme
- ☒ Liste des destinataires des données
- ☒ Documentation des interfaces et des programmes de consultation et de transmission

Pour les impressions et les supports de données :

- ☒ Effectuer des contrôles d'inventaire réguliers
- ☐ Sélection minutieuse du personnel et des véhicules de transport (n'est pas applicable)
- ☐ Sûreté des transports liée à l'occasion (par exemple, conteneurs, cryptage des supports de stockage, protocoles de transfert) (n'est pas applicable)

Divers :

Contrôle des entrées

La traçabilité et la documentation de la gestion et de la maintenance des données doivent être assurées.

Les mesures de vérification ultérieure visant à déterminer si des données ont été introduites, modifiées ou supprimées (effacées) et par qui :

- ☒ Enregistrement des entrées et vérification des journaux
- ☒ Traçabilité de la saisie, de la modification et de la suppression des données grâce à des noms d'utilisateur individuels (pas de groupes d'utilisateurs)
- ☒ Conservation des formulaires dont les données ont été reprises dans un traitement automatisé
- ☒ Octroi de droits d'entrée, de modification et de suppression de données sur la base d'un concept d'autorisation
- ☒ Responsabilités organisationnelles pour la saisie

Divers :

3. Disponibilité et résilience (art. 32, alinéa 1, lettres b) et c) du RGPD)

Contrôle de disponibilité

Les données doivent être protégées contre toute destruction ou perte accidentelle.

Mesures de protection des données (physiques/logiques) :

☒ Contrôle régulier de l'état du système (monitoring)

☒ Rétablissement à court terme de l'état normal du système

Concept de sauvegarde et de redémarrage (sauvegardes régulières des données) :

☐ hors ligne ☒ en ligne ☒ sur site ☐ hors site ☐

☒ Concept d'archivage des données

☒ Existence d'un concept d'urgence ((Business Continuity, Disaster Recovery (continuité des activités, reprise après sinistre))

☒ Tests réguliers du concept d'urgence

☒ Existence de systèmes informatiques redondants (par exemple, serveur, stockage)

☒ Reproductibilité des machines virtuelles

☒ Équipement de protection physique opérationnel (protection contre l'incendie, énergie : alimentation sans interruption (ASI), climat)

☒ Canaux de notification et plans d'urgence

Divers :

Vérification de la capacité de charge

Le traitement des données doit être tolérant aux perturbations et aux erreurs.

- ☒ Protection anti-virus/anti-malware/anti-ransomware
- ☒ capacité de réseau généreusement disponible
- ☒ matériel renforcé en particulier contre les attaques DoS et DDoS
- ☐ IDS/IPS
- ☒ Architecture de système adaptée/DMZ
- ☒ Pare-feu

4. Procédures d'examen, d'appréciation et d'évaluation périodiques

(article 32, alinéa 1, lettre d) du RGPD ; article 25, alinéa 1 du RGPD)

☒ Règlements écrits sur les responsabilités en matière de protection des données

☒ Réglementation écrite des responsabilités en matière de sécurité de l'information

☒ Existence d'un système approprié de gestion de la sécurité de l'information

☒ Existence d'une gestion appropriée de la réponse aux incidents (Incident Response Management)

☒ Mise en œuvre d'une classification des informations

☒ Éducation et sensibilisation régulières des employés et des cadres

☒ Paramètres par défaut favorables à la protection des données (article 25, alinéa 2, du RGPD) ;

Contrôle des commandes pour s'assurer que les commandes soient traitées conformément aux instructions :

☒ Respect strict des accords stipulés et des contrôles y afférents

☒ Concept de suivi régulier du processus de commande (par exemple, présentation d'auto-évaluations, présentation des contrats avec les sous-traitants du Sous-traitant, mise en œuvre de contrôles chez les sous-traitants par le contractant)

☒ Pas de traitement de données sur commande au sens de l'article 28 du RGPD sans instructions correspondantes du Mandant, par exemple sur la base de : conception claire du contrat, gestion formalisée de la commande, sélection stricte du prestataire de services, obligation de convaincre à l'avance, contrôles de suivi.

Divers :

Annexe 2

Désignation du délégué à la protection des données, de la personne de contact ou du représentant au sein de l'Union européenne conformément à l'article 16 de l'accord ST

Le Sous-traitant désigne :

En tant que délégué à la protection des données, le Dr Timo Hoffmann

Adresse : Eckweg 1, 78048 Villingen-Schwenningen

Courrier électronique : timo.hoffmann@hub24.de

En tant que personne de contact, M. Frank Korthouwer

Adresse : Kabelweg 57, 1014 BA Amsterdam

Tél. : +31 23 3000000

Courrier électronique : frank.korthouwer@idiligo.com

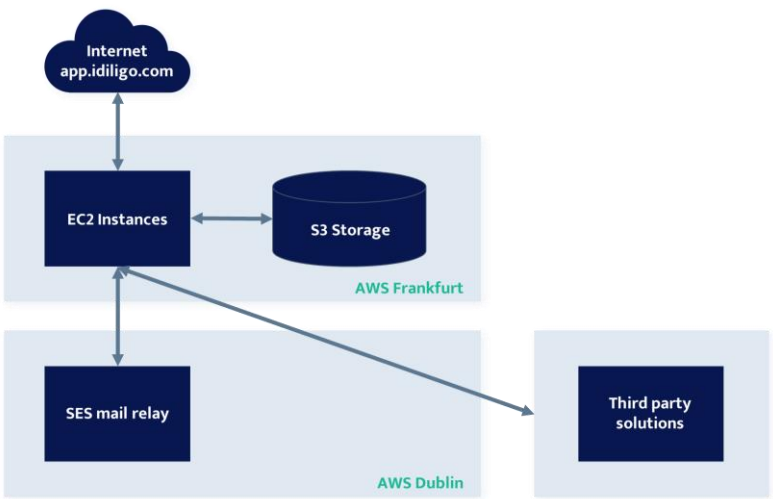
Annexe 3

Relation de sous-traitance avec le Sous-traitant au moment de l'attribution du contrat

Nom du sous-traitant du Sous-traitant	Description des services partiels	Lieu d'exécution
Amazon (AWS)	Stockage des données dans la mémoire d'Amazon S3. Tant EC2 que S3	Francfort, Allemagne
Amazon (AWS)	Fonction de relais de courrier SES	Dublin, Irlande
Intelligence numérique (Digital Intelligence)	Développement de l'application Idiligo	Amsterdam, Pays-Bas
The Rocket Science Group LLC d/b/a Mailchimp	Informations sur les clients par courrier électronique	Pays tiers, UE
Exact	Envoi des factures	UE
Intelligent Solution Services AG	Signature numérique	Stuttgart, Allemagne

Gestion et architecture de la sécurité

- L'Elastic Compute Cloud (EC2) d'Amazon offre une fonctionnalité appelée Groupes de sécurité (Security Groups), qui est similaire à un pare-feu de réseau entrant dans lequel Idiligo spécifie les protocoles, les ports et les plages d'IP source que les instances EC2 sont autorisées à atteindre.Stockage et sauvegardes
- Les documents téléchargés ou générés pour être utilisés lors de réunions interactives d'Idiligo sont stockés dans le S3. Les données sont stockées cryptées avec le Key Management Service (KMS) d'AWS.Idiligo met en place une sauvegarde quotidienne des informations spécifiques aux clients avec un historique maximum de 8 jours dans un environnement Amazon S3 séparé.



Annexe 4

Lieux de service convenus conformément à l'article 7 de l'accord

Nom et adresse du Sous-traitant	Nom et adresse du sous-traitant du Sous-traitant	Lieu d'exécution des services
Idiligo B.V. Kabelweg 57, 1014 BA Amsterdam, Pays-Bas	Amazon (AWS) Francfort	Allemagne