Annexe 2 - Contrat de traitement de données à caractère personnel sur mandat conformément à l'article 28, paragraphe 3, du RGPD

_____

entre

le client

- ci-après dénommée "**commanditaire**" -

et

Timly Software AG, Andreasstrasse 5, 8050 Zurich, Suisse

- ci-après dénommé "**le sous-traitant**" -

ensemble, les "**parties**".

1. Objet du marché

1.1 Dans le cadre de l'exécution du contrat de prestation, il est nécessaire que le sous-traitant traite des données à caractère personnel pour lesquelles le commanditaire agit en tant que responsable au sens de l'article 4, point 7 du RGPD (ci-après dénommées "données du commanditaire"). Le présent contrat contient les dispositions, notamment les droits et obligations des parties en matière de protection des données, relatives au traitement des données du donneur d'ordre par le sous-traitant pour l'exécution du contrat de prestation. Le mandat comprend les prestations décrites dans le contrat de prestations.

1.2 Sans préjudice du paragraphe 3, le sous-traitant traite les données à caractère personnel exclusivement dans un État membre de l'Union européenne ou dans un État partie à l'accord sur l'Espace économique européen.

1.3 Si le sous-traitant traite des données à caractère personnel dans un pays tiers (c'est-à-dire en dehors de l'Union européenne/d'un État signataire de l'accord sur l'Espace économique européen), cela nécessite l'accord écrit préalable du donneur d'ordre et n'a lieu que si et dans la mesure où les conditions particulières des articles 44 et suivants du RGPD sont remplies.

2. Informations sur le contenu de la mission

2.1 Le sous-traitant traite les données du donneur d'ordre exclusivement sur mandat (§ 1, alinéa 1 du présent contrat) et selon les instructions documentées du donneur d'ordre au sens de l'article 28, alinéa 3, lettre a du RGPD.

2.2 Le sous-traitant traite les données du donneur d'ordre exclusivement de la manière, dans l'étendue et aux fins qui sont définitivement nécessaires à la fourniture des prestations conformément au contrat de prestations. Tout traitement des données du donneur d'ordre qui s'écarte ou dépasse ce cadre est interdit au sous-traitant, en particulier l'utilisation des données du donneur d'ordre à des fins personnelles.

2.3 Le sous-traitant traite en outre les données suivantes qui méritent d'être protégées, telles que les données de communication (par ex. téléphone, e-mail), les données de base du contrat (relation contractuelle, intérêt du produit ou du contrat), l'historique du commanditaire, les données de facturation et de paiement du contrat, les données de planification et de contrôle, les données de renseignement (provenant de tiers, par ex. d'agences de renseignements, ou d'annuaires publics) ainsi que les noms, prénoms et adresses e-mail dans la mesure où ils sont enregistrés par le commanditaire.

2.4 Les catégories de personnes concernées par le traitement du côté du donneur d'ordre comprennent les commanditaires, les prospects, les abonnés, les employés, les fournisseurs, les agents commerciaux, les personnes de contact. Le sous-traitant documente le traitement des catégories de traitement dans un registre au sens de l'article 28, paragraphe 2, et le met à la disposition du donneur d'ordre de manière appropriée sur demande.

3. Pouvoir d'instruction du donneur d'ordre, traitement sur instructions

3.1 Le donneur d'ordre donne toutes les instructions et commandes par écrit ou dans un format électronique documenté. Si le donneur d'ordre donne une instruction oralement, celle-ci doit être confirmée immédiatement par le donneur d'ordre par écrit ou dans un format électronique documenté. Le donneur d'ordre dispose d'un droit général d'instruction vis-à-vis du sous-traitant en ce qui concerne le type, l'étendue et la méthode de traitement des données.

3.2 Les données ne peuvent être traitées que conformément aux dispositions du présent accord et aux instructions du donneur d'ordre. Il est interdit au sous-traitant d'utiliser les données à d'autres fins et, en particulier, de les divulguer à des tiers. Aucune copie ou duplication ne peut être effectuée à l'insu du donneur d'ordre. Sont exclues de cette disposition les copies de sauvegarde, dans la mesure où elles sont nécessaires pour garantir le traitement correct des données, ainsi que toutes les données nécessaires au respect des obligations légales de conservation.

3.3 Toute modification de l'objet et de la procédure du traitement doit faire l'objet d'un accord commun et être documentée. Le sous-traitant ne peut transmettre les données à caractère personnel traitées dans le cadre du présent accord à des tiers ou à la personne concernée qu'avec l'accord écrit préalable du commanditaire.

3.4 Si le sous-traitant estime qu'une instruction du donneur d'ordre enfreint les dispositions légales en matière de protection des données, il doit en informer le donneur d'ordre sans délai. Il peut alors suspendre l'exécution de l'instruction en question jusqu'à ce qu'elle soit confirmée ou modifiée par le représentant du donneur d'ordre.

4. Droits et obligations du commanditaire

4.1 Le donneur d'ordre est seul responsable vis-à-vis de l'extérieur, en particulier vis-à-vis des tiers et des personnes concernées, de l'évaluation de la licéité du traitement des données à caractère personnel conformément à l'article 6, paragraphe 1, du RGPD et du respect des droits des personnes concernées conformément aux articles 12 à 22 du RGPD. Le sous-traitant est néanmoins tenu, dans la mesure où la loi l'autorise, de transmettre au donneur d'ordre toutes les demandes des personnes concernées, dans la mesure où elles s'adressent visiblement au donneur d'ordre. Le sous-traitant aide le commanditaire dans une mesure raisonnable à répondre aux demandes des personnes concernées (par ex. rectification, effacement et blocage des données) et est en droit de facturer une indemnité raisonnable à cet effet.

4.2 Le donneur d'ordre est le propriétaire des données du donneur d'ordre et, dans les relations entre les parties, le propriétaire de tous les droits éventuels sur les données du donneur d'ordre.

4.3 Il incombe au donneur d'ordre de mettre les données du donneur d'ordre à la disposition du sous-traitant en temps utile pour la fourniture de la prestation conformément au contrat de prestation. En outre, le commanditaire est responsable de la qualité et de la légalité de la collecte des données du commanditaire. Le donneur d'ordre doit informer immédiatement et complètement le sous-traitant s'il constate, lors de l'examen des résultats de la commande du sous-traitant, des erreurs ou des irrégularités concernant les dispositions légales sur la protection des données ou ses instructions.

4.4 Dans le cas où un tiers ou une personne concernée fait valoir une prétention directement à l'encontre du sous-traitant en raison d'une violation des droits de la personne concernée et/ou de prétentions y afférentes, le donneur d'ordre s'engage à indemniser le sous-traitant de tous les dommages, coûts/frais, y compris les frais d'avocat, ou autres dépenses ou pertes, qui découlent de la réclamation, si et dans la mesure où le sous-traitant a informé le commanditaire de l'exercice de la réclamation, que cette violation n'est pas due à des traitements effectués en violation des instructions du commanditaire et qu'il lui a donné la possibilité de coopérer avec le sous-traitant dans le cadre de la défense de la réclamation.

5. Obligations du sous-traitant

5.1 Le sous-traitant est tenu de traiter les données à caractère personnel exclusivement dans le cadre des accords conclus et conformément aux instructions du donneur d'ordre. Cette disposition ne s'applique pas si le sous-traitant est tenu de procéder à un autre traitement en vertu du droit de l'Union ou des États membres auquel le sous-traitant est soumis (par exemple, enquêtes menées par les autorités de l'État, les services répressifs). Dans ce cas, le sous-traitant communique ces exigences légales au commanditaire avant le traitement, à moins que le droit concerné n'interdise une telle communication en raison d'un intérêt public important (cf. article 28, paragraphe 3, phrase 2, point a) du RGPD).

5.2 Le sous-traitant n'utilise pas les données à caractère personnel fournies par le commanditaire pour le traitement à d'autres fins, notamment à ses propres fins. Le sous-traitant n'est pas autorisé à faire des copies ou des duplications des données du donneur

d'ordre sans l'accord écrit préalable du donneur d'ordre, dans la mesure où et aussi longtemps que cela n'est pas nécessaire pour garantir un traitement correct des données, pour fournir correctement les prestations conformément au contrat de prestations (y compris la sauvegarde des données) ou pour respecter les obligations légales de conservation.

5.3 Le sous-traitant ne peut pas non plus transmettre les données du commanditaire à des tiers ou à d'autres destinataires sans l'accord écrit préalable du commanditaire. Font exception à cette règle les transmissions de données à des sous-traitants dont le commanditaire a approuvé la mission.

5.4 Dans la mesure où la loi l'autorise, le sous-traitant ne fournit à des tiers ou à des autorités des informations sur les données à caractère personnel issues de la présente relation de travail qu'après avoir reçu des instructions ou l'accord préalable du commanditaire, par écrit ou sous forme de document électronique.

5.5 Si le donneur d'ordre est tenu de fournir des informations sur les données du donneur d'ordre ou sur leur traitement à une autorité publique, à une personne concernée ou à une autre personne, le sous-traitant est tenu d'aider le donneur d'ordre à fournir de telles informations à la première demande, notamment en mettant à disposition sans délai toutes les informations et tous les documents relatifs au traitement des données du donneur d'ordre faisant l'objet du contrat, y compris les mesures techniques et organisationnelles prises par le sous-traitant, le déroulement technique de l'utilisation des données du donneur d'ordre, les lieux où les données du donneur d'ordre sont utilisées et les collaborateurs impliqués dans le traitement.

5.6 Le sous-traitant s'engage à coopérer dans la mesure nécessaire à l'exercice des droits des personnes concernées conformément aux articles 12 à 22 du RGPD, à l'établissement des registres des activités de traitement, aux évaluations d'impact sur la protection des données requises par le donneur d'ordre, ainsi qu'au respect des obligations du donneur d'ordre en matière de sécurité du traitement et, dans la mesure du possible, à apporter un soutien approprié au donneur d'ordre (cf. article 28, paragraphe 3, phrase 2, lettres e, f du RGPD).

5.7 Le sous-traitant est tenu de rectifier, d'effacer ou de limiter le traitement des données à caractère personnel issues de cette relation contractuelle si le commanditaire l'exige au moyen d'instructions écrites ou documentées par voie électronique et si les intérêts légitimes du sous-traitant, notamment le respect des dispositions légales, ne s'y opposent pas.

5.8 Le donneur d'ordre et le sous-traitant se concertent pour procéder à une modification de l'objet du traitement ou à un changement de procédure. La modification est consignée par écrit ou dans un format électronique documenté.

5.9 Pour les actes d'assistance visés au présent article 5, le sous-traitant est en droit de facturer une indemnité appropriée.

5.10 Après l'achèvement des travaux convenus par contrat ou plus tôt à la demande du commanditaire - au plus tard à la fin de l'accord de prestation - le preneur d'ordre doit, au choix du commanditaire, remettre à ce dernier tous les documents, résultats de traitement et d'utilisation produits ainsi que les fichiers de données en rapport avec la relation contractuelle ou, après accord préalable, les détruire en respectant la protection des données. Il en va de même pour le matériel de test et de rebut. Le procès-verbal de la

suppression doit être présenté sur demande. Les documentations qui servent à prouver que le traitement des données est conforme à la commande et à la réglementation doivent être conservées par le commanditaire au-delà de la fin du contrat, conformément aux délais de conservation respectifs. Il peut les remettre au commanditaire à sa décharge à la fin du contrat.

6. Mesures techniques et organisationnelles

6.1 Le sous-traitant est tenu de mettre en œuvre et de maintenir pendant la durée du contrat les mesures techniques et organisationnelles nécessaires pour assurer, dans le cadre du traitement concret des données, un niveau de protection approprié au regard des risques pour les droits et libertés des personnes physiques concernées par le traitement. Les objectifs de protection de l'article 32, paragraphe 1, du RGPD, tels que la confidentialité, l'intégrité et la disponibilité des systèmes et services, ainsi que leur résilience au regard de la nature, de l'ampleur, des circonstances et des finalités des traitements, sont pris en compte afin de réduire au maximum tout risque pendant la durée du contrat.

6.2 Le concept de protection des données du sous-traitant (mesures techniques et organisationnelles (TOM)) de Timly Software AG présente de manière détaillée le choix des mesures adaptées au risque identifié, en tenant compte des objectifs de protection selon l'état de l'art et en tenant compte en particulier des systèmes informatiques et des processus de traitement mis en œuvre chez le sous-traitant. Le donneur d'ordre confirme que les mesures techniques et organisationnelles offrent un niveau de protection adéquat pour les données du donneur d'ordre, compte tenu des risques liés au traitement de ces données.

6.3 Les mesures techniques et organisationnelles sont soumises au progrès technique et au développement. Dans cette mesure, le sous-traitant est autorisé à mettre en œuvre des mesures alternatives adéquates. Ce faisant, le niveau de sécurité des mesures définies ne doit pas être inférieur. Les modifications importantes doivent être documentées.

7. Rectification, effacement et verrouillage des données

7.1 Le sous-traitant ne peut rectifier, effacer ou bloquer les données traitées pour le compte du donneur d'ordre que sur instruction de ce dernier.

7.2 Si une personne concernée s'adresse directement au sous-traitant pour obtenir la rectification ou l'effacement de ses données à caractère personnel, le sous-traitant transmettra cette demande au commanditaire.

8. Contrôles et autres obligations du sous-traitant

Le sous-traitant respectera les exigences suivantes :

a) Si la loi le prévoit, le sous-traitant désigne par écrit un délégué à la protection des données qui exerce son activité conformément aux dispositions légales. Le délégué à la protection des données est désigné auprès du sous-traitant (Actuellement non prévu par la loi). Tout changement de délégué à la protection des données doit être immédiatement communiqué au donneur d'ordre.

b) Le sous-traitant et toute personne placée sous l'autorité du sous-traitant qui a accès aux données à caractère personnel du commanditaire ne peuvent traiter ces données que conformément aux instructions du commanditaire visées à l'article 9 du présent contrat, y compris les pouvoirs accordés par le présent contrat, à moins qu'ils ne soient tenus de les traiter en vertu du droit de l'Union européenne ou des États membres auquel le sous-traitant est soumis. Dans un tel cas, le sous-traitant notifie ces exigences légales au commanditaire, à moins que le droit concerné n'interdise une telle notification en raison d'un intérêt public important.

c) Le sous-traitant ne fait appel, pour l'exécution des travaux, qu'à des personnes qui se sont engagées à respecter la confidentialité et qui ont été préalablement familiarisées avec les dispositions relatives à la protection des données qui les concernent.

d) Les donneurs d'ordre et les sous-traitants coopèrent, sur demande, avec l'autorité de contrôle dans l'accomplissement de leurs tâches.

e) Le sous-traitant informe immédiatement le donneur d'ordre des actes de contrôle et des mesures prises par l'autorité de contrôle, dans la mesure où ils se rapportent à cette mission. Il en va de même dans la mesure où une autorité compétente enquête dans le cadre d'une procédure d'infraction ou d'une procédure pénale concernant le traitement de données à caractère personnel effectué par le sous-traitant dans le cadre de la sous-traitance.

f) Le sous-traitant assiste le commanditaire dans la mesure où le commanditaire est soumis à un contrôle de l'autorité de contrôle, à une procédure d'infraction ou à une procédure pénale, à l'action en responsabilité d'une personne concernée ou d'un tiers ou à toute autre action en relation avec le traitement des données à caractère personnel effectué chez le sous-traitant.

g) Le sous-traitant contrôle régulièrement ses processus internes, ainsi que les mesures techniques et organisationnelles, afin de garantir que le traitement dans son domaine de responsabilité est effectué conformément aux exigences de la législation applicable en matière de protection des données et que la protection des droits de la personne concernée est assurée.

h) Le sous-traitant apporte la preuve des mesures techniques et organisationnelles prises vis-à-vis du donneur d'ordre dans le cadre de ses pouvoirs de contrôle conformément au point 7 du présent contrat.

9. Relations de sous-traitance

9.1 Aux fins de la présente réglementation, on entend par relations de sous-traitance les services qui se rapportent directement à la fourniture de la prestation principale. En sont exclues les prestations annexes auxquelles le sous-traitant fait appel, par exemple sous la forme de services de télécommunication, de services postaux/de transport ou d'élimination de supports de données. Le sous-traitant est toutefois tenu de prendre des dispositions contractuelles appropriées et conformes à la loi ainsi que des mesures de contrôle pour garantir la protection des données et la sécurité des données du donneur d'ordre, même en cas de prestations annexes externalisées.

9.2 Pour l'exécution du contrat, le sous-traitant est autorisé à faire appel aux sous-traitants secondaires énumérés à l'appendice 3 pour le traitement des données à caractère personnel. Le recours à d'autres sous-traitants ou à d'autres sous-traitants pour le traitement des données à caractère personnel du donneur d'ordre n'est autorisé qu'après avoir informé préalablement le donneur d'ordre par écrit de l'identité du sous-traitant et de l'objet de la sous-traitance, à moins que le donneur d'ordre ne s'oppose à cette modification dans un délai raisonnable d'au moins 10 jours ouvrables. Par ailleurs, les dispositions suivantes s'appliquent :

a) La transmission de données à caractère personnel du donneur d'ordre au sous-traitant ultérieur et la première intervention de ce dernier ne sont autorisées que lorsque toutes les conditions requises pour une sous-traitance ultérieure sont remplies.

b) Si le sous-traitant ultérieur fournit la prestation convenue avec l'accord du commanditaire conformément au point 2.1 en dehors de l'UE/EEE, le sous-traitant s'assure de la licéité en matière de protection des données conformément aux dispositions légales relatives à la protection des données applicables à l'exécution du contrat.

c) Le sous-traitant ultérieur doit se voir imposer, par voie contractuelle, les mêmes obligations en matière de protection des données que celles énoncées dans le présent contrat, en fournissant notamment des garanties suffisantes que les mesures techniques et organisationnelles appropriées seront mises en œuvre de manière à ce que le traitement soit effectué conformément aux exigences légales.

10. Droits de contrôle du commanditaire

10.1 Le donneur d'ordre a le droit de procéder à des contrôles en concertation avec le sous-traitant ou de les faire effectuer par des contrôleurs tenus au secret professionnel et à désigner au cas par cas. Il a le droit de s'assurer du respect du présent accord par le sous-traitant dans ses activités commerciales en procédant à des contrôles aléatoires qui doivent être annoncés en temps utile. Le sous-traitant peut exiger un dédommagement approprié pour les dépenses qu'il a engagées (par ex. heures de travail des collaborateurs engagés).

10.2 Le sous-traitant veille à ce que le commanditaire puisse s'assurer du respect des obligations légales et contractuelles du sous-traitant. Le sous-traitant s'engage à fournir au donneur d'ordre, à sa demande, les informations nécessaires et notamment à prouver la mise en œuvre des mesures techniques et organisationnelles.

10.3 La preuve de telles mesures, qui ne concernent pas uniquement la commande concrète, peut être apportée par des attestations actuelles, des rapports ou des extraits de rapports d'instances indépendantes (par ex. commissaires aux comptes, audit, délégué à la protection des données, département de sécurité informatique, auditeurs de protection des données, auditeurs de qualité), des certifications appropriées (audit de sécurité informatique ou de protection des données, par ex. selon BSI-Grundschutz) ou d'autres mesures prévues par la loi.

11. Assistance au donneur d'ordre, notification des infractions commises par le sous-traitant

Le sous-traitant aide le commanditaire à respecter ses obligations légales en matière de protection et de sécurité des données à caractère personnel et le documente de manière appropriée. Il s'agit notamment

a) assurer un niveau de protection adéquat par des mesures techniques et organisationnelles qui tiennent compte des circonstances et des finalités du traitement, ainsi que de la probabilité et de la gravité prévues d'une éventuelle violation de la loi par des failles de sécurité, et qui permettent de détecter immédiatement les événements de violation pertinents,

b) l'obligation de documenter les violations de la protection des données à caractère personnel et de les notifier immédiatement au donneur d'ordre. Le sous-traitant doit, en accord avec le donneur d'ordre, prendre les mesures appropriées pour sécuriser les données et minimiser les effets potentiellement négatifs sur les personnes concernées,

c) l'obligation d'assister le commanditaire par des mesures appropriées, dans la mesure où le commanditaire doit informer l'autorité de contrôle compétente ou la personne concernée de la violation de la protection des données à caractère personnel,

d) l'obligation d'assister le commanditaire dans le cadre de son devoir d'information vis-à-vis de la personne concernée et, dans ce contexte, de lui fournir immédiatement, à sa demande, toutes les informations pertinentes.

12. Divers et dispositions finales

12.1 La durée du présent contrat correspond à la durée du contrat de prestations. Les dispositions relatives à la résiliation ordinaire du contrat de prestations s'appliquent par analogie. La résiliation du contrat de prestations entraîne automatiquement la résiliation du présent contrat. Une résiliation isolée du présent contrat est exclue.

12.2 Si une disposition actuelle ou future du contrat est ou devient totalement ou partiellement invalide ou inapplicable, ou si le présent contrat présente une lacune, la validité des autres dispositions n'en sera pas affectée. La disposition invalide ou inapplicable est remplacée par la disposition valide qui se rapproche le plus du sens et de l'objectif économique de la disposition invalide ou inapplicable. En cas de lacune dans la réglementation, la disposition convenue est celle qui correspond à ce qui aurait été

convenu selon le sens et le but économiques de la présente convention si les parties avaient d'emblée tenu compte de la lacune.

12.3 Les parties s'engagent à modifier et/ou à compléter le présent accord à la demande de l'une des parties si cela s'avère nécessaire en raison d'une modification des lois sur la protection des données applicables aux parties ou parce que la Commission européenne et/ou les autorités de contrôle compétentes pour les parties indiquent, par des avis généraux ou des publications (par exemple par la mise à disposition de clauses contractuelles types conformément à l'art. 28, al. 7, al. 8 du RGPD) ou sous la forme de déclarations ou d'injonctions dans des cas particuliers, que le présent accord dans sa forme existante ne satisfait pas aux exigences des lois sur la protection des données applicables.

Etat 02/2022, Timly Software AG

datenschutz@timly.ch