Accord pour un Traitement des données de commande

conclu entre

les utilisateurs des services de commande et d'établissement d'ordonnances électroniques et d’autres services informatiques de Zur Rose
(le «client» / responsable)

et

Zur Rose Suisse SA
Walzmühlestrasse 60
8500 Frauenfeld
(le «prestataire» / sous-traitant)

1 Objet et champ d'application

1.1 Le présent accord de sous-traitance («accord ST») s'applique lorsque le sous-traitant traite des données pour le compte du client («accord de base»), en particulier en rapport avec des produits et services informatiques. Il concrétise les obligations des parties relevant du droit de la protection des données, qui découlent de la sous-traitance décrite dans l'accord de base et des fonctions d'un produit informatique.

1.2 Toutes les obligations décrites dans le présent accord ST s'appliquent à toutes les activités en rapport avec l'accord de base dans lesquelles le prestataire, ses collaborateurs et les tiers auxquels il recourt utilisent des données à caractère personnel du client (les «données personnelles»). Si des dispositions de l'accord ST contredisent des dispositions de l'accord de base, les dispositions de l'accord ST prévalent dans tous les cas.

1.3 **Restriction du champ d'application**: Le présent accord ST ne s'étend pas au traitement des coordonnées du client ou de ses collaborateurs dans les propres finalités du prestataire, au traitement des ordonnances et à d'autres traitements de données par Zur Rose Suisse SA dans sa fonction de pharmacie. De tels traitements sont effectués par Zur Rose Suisse SA elle-même en tant que responsable.

1.4 Le prestataire traite les données personnelles pour le compte du client conformément aux prestations convenues dans l'accord de base. Le traitement peut porter sur les données personnelles suivantes:

- **Traitements de données entrepris:** découlent de l'accord de base
- **Catégories de données concernées:** en particulier données personnelles de base (par exemple collaborateurs, patients, clients); données de santé; données de contact et de communication (téléphone, e-mail, adresses IP, etc.); données contractuelles (par exemple relations contractuelles, intérêt pour des produits); historiques des clients; données de décompte et de paiement; données de planification et de gestion, etc.
- **Données personnelles sensibles:** en particulier données médicales des patients (par exemple résultats, documentation médicale, diagnostics, médicaments, documents, etc.); données sur la sphère intime, etc.
- **Catégories de personnes concernées:** Patients, clients, personnes intéressées, collaborateurs, fournisseurs et partenaires commerciaux, etc.

2 Responsabilités et garantie

2.1 Dans le cadre du présent accord ST et des directives données, le client, en tant que «responsable», répond envers les tiers de la légalité du traitement des données et du respect des obligations d'information légales.

2.2 Le prestataire garantit qu'il a tenu ses collaborateurs et les tiers auxquels ils recourent à la confidentialité ou que ceux-ci sont soumis à une obligation légale de garder le secret. De plus, il a attiré leur attention sur le fait que l'obligation de confidentialité perdure au-delà de la fin de leur activité.

3 Pouvoir de donner des instructions du client

3.1 Le prestataire traite les données personnelles uniquement dans le cadre de ce qui est convenu et sur instruction du client. En sont exclus les situations dans lesquelles le prestataire est tenu d'effectuer un traitement pour des motifs juridiques impérieux. Dans de telles situations, le prestataire informe le client de ces exigences légales avant le début du traitement, dans la mesure où cela est autorisé.

3.2 Dans le cadre du présent accord ST, le client dispose d'un droit de donner des instructions sur la nature, l'étendue et la procédure du traitement des données, qu'il peut concrétiser ou compléter par des instructions individuelles. Le prestataire informe le client s'il pense qu'une instruction enfreint des lois applicables (sachant qu'il n'est tenu à aucune obligation de vérification). Il peut suspendre l'application de l'instruction jusqu'à ce que celle-ci ait été confirmée ou modifiée par le client en clarifiant la responsabilité.

4 Lieu du traitement des données

Le prestataire et les tiers auxquels il recourt traitent des données personnelles en Suisse, dans un pays membre de l'Union européenne (UE) ou dans un pays ayant ratifié l'Accord sur l'Espace Économique Européen (EEE). Si le prestataire recourt à un tiers en dehors de ce territoire, il est responsable du respect des exigences légales concernant la garantie d'un niveau de sécurité adéquat. Le chiffre 7 demeure réservé.

5 Obligations du prestataire

5.1 **Traitement des données:** Le prestataire s'engage à traiter les données personnelles et les résultats du traitement uniquement dans le cadre des instructions du client. Si le prestataire reçoit l'ordre d'une autorité de communiquer des données du client, si cela est admis, il doit en informer immédiatement le client et renvoyer l'autorité vers celui-ci.

5.2 **Mesures de sécurité:** Le prestataire conçoit son organisation de manière à ce qu'elle satisfasse aux exigences particulières de la protection des données. Il prend toutes les mesures techniques et organisationnelles adaptées au risque et conformes à l'état de la technique afin de garantir la confidentialité, la disponibilité et l'intégrité des données personnelles, la possibilité de suivi du traitement et la résistance de ses prestations de services s'y rapportant, en respectant au moins les mesures de sécurité consignées dans l'annexe 1. Sur demande, il prouve ces mesures et leur mise en œuvre au client et aux autorités de surveillance.

5.3 **Étude d'impact de la protection des données:** Si le client doit réaliser une étude d'impact de la protection des données, le prestataire fournit, eu égard aux traitements de données personnelles qu'il effectue pour le client, les faits et informations techniques requis pour l'étude d'impact et assiste le client comme il se doit dans les consultations des autorités de surveillance.

5.4 **Obligations d'assistance:** Le prestataire apporte son concours au client dans le respect de ses obligations légales relatives à la protection des données (par exemple mesures de sécurité des données, notifications de violations à l'autorité de surveillance, information de la personne concernée par une violation). En particulier, le prestataire instruit le client dans les plus brefs délais au sujet de toutes les infractions à des prescriptions ou des instructions qui ont été portées à sa

connaissance et prend toutes les mesures requises pour garantir et limiter les possibles conséquences préjudiciables pour les personnes concernées.

5.5 **Droits des personnes concernées:** Le prestataire prend les mesures techniques et organisationnelles pour que le client puisse respecter au cas par cas et dans les délais prescrits les droits des personnes concernées conformément à la législation sur la protection des données en vigueur, en particulier information, accès, rectification et effacement (ou anonymisation), portabilité des données, opposition et décisions automatisées, et remet au client toutes les informations nécessaires à cet effet. Si une demande en ce sens est soumise au prestataire, celui-ci la transmettra dans les plus brefs délais au client pour qu'il la traite.

5.6 **Obligation d'effacement et de remise:** Le prestataire rectifie, efface (ou anonymise) ou bloque des données personnelles uniquement sur instruction du client et garantit des processus conformes à la protection des données. Les obligations d'information et de remise demeurent réservées. À la fin du contrat ou sur demande du client, le prestataire doit remettre au client certains ou tous les résultats du traitement et documents qui contiennent des données personnelles ou, selon ce qui est convenu, les détruire pour son compte, sous réserve d'un enregistrement temporaire des données personnelles dans des systèmes de sauvegarde et d'archivage jusqu'à leur prochain effacement ordinaire (le présent accord ST demeure applicable pour ces données personnelles). Si le prestataire traite les données dans un format technique spécial, il est tenu, en contrepartie d'une indemnisation appropriée, de transmettre les données soit dans ce format soit, si le client le souhaite, dans un autre format courant qui permette de transférer les données dans une nouvelle application avec le moins de pertes possible et en conservant la structure des données et la logique.

5.7 **Procès-verbaux** Si des données sensibles sont traitées de façon automatisée à grande échelle ou si un profilage est établi avec un risque élevé, le client en informe le prestataire et celui-ci doit au moins consigner l'enregistrement, la modification, la lecture, la communication l'effacement et la destruction des données dans un procès-verbal. Le procès-verbal doit renseigner sur l'identité de la personne qui a effectué le traitement, la nature, la date et l'heure du traitement ainsi que, le cas échéant, l'identité du destinataire des données. Les procès-verbaux doivent être conservés pendant au moins un an, séparément du système dans lequel les données personnelles sont traitées. L'accès aux procès-verbaux est réservé exclusivement aux organes et personnes chargés de vérifier l'application des prescriptions relatives à la protection des données ou de sauvegarder ou rétablir la confidentialité, de l'intégrité, de la disponibilité et du suivi des données et ils ne peuvent être utilisés qu'à cet effet.

5.8 **Obligation de contrôle**: Le prestataire contrôle et documente le respect des obligations précitées.

6 Sauvegarde du secret professionnel

6.1 Le prestataire peut également traiter des données ou accéder à des données qui relèvent du secret professionnel au sens de l'art. 321 du Code pénal (CP) et dont la divulgation non autorisée peut être sanctionnée. Le prestataire s'engage à garder le silence sur les secrets professionnels et à ne prendre connaissance de ces données que dans la mesure nécessaire à l'accomplissement des tâches qui lui ont été confiées ou dans la mesure où le client lui transmet ces données.

Le cas échéant, le prestataire doit faire usage du droit de refuser de témoigner prévu à l'art. 171 CP et de l'interdiction de séquestre prévue à l'art. 262 CP.

6.2 Le prestataire s'assure que tous les collaborateurs et tiers auxquels il recourt se sont engagés par écrit à ne pas divulguer des secrets professionnels auxquels ils ont accès et ont confirmé qu'ils ont été informés d'une éventuelle punissabilité prévue par le CP et la loi sur la protection des données (LPD).

6.3 Le prestataire doit sélectionner minutieusement les éventuels sous-traitants et les obliger à garder le silence sur les données soumises au secret professionnel, dans la mesure où ils y ont accès. De plus, ces sous-traitants doivent obliger par écrit le personnel employé à respecter la confidentialité et à les informer des conséquences d'une violation de leur obligation. Cette disposition est valable de la même manière pour tous les autres sous-traitants.

7 Rapports de sous-traitance

7.1 Si, pour le traitement des données personnelles, le prestataire sollicite des prestations de tiers qui traitent les données personnelles pour son compte («sous-traitants»), le prestataire tient la liste suivante répertoriant leurs noms, adresses et domaines d'activité.

Nom/adresse	Domaine d'activité	Lieu du traitement des données
Clustertec AG, Baarmattstrasse 10, 6340 Baar	Développement d'applications	Baar
BlueCare AG, Pflanzschulstrasse 3, 8400 Winterthour	Onboarding de clients, support de premier niveau	Winterthour

7.2 Le recours éventuel à d'autres sous-traitants doit être notifié par écrit au client. Un tel recours est considéré comme accepté s'il n'y est pas fait opposition par écrit dans un délai de 30 jours.

8 Obligations d'information et droits d'audit

8.1 En cas de violation de la sécurité des données, le prestataire en informe le client dans les plus brefs délais. Il apporte son concours au client dans le traitement et prépare les documents auxquels il a accès. Ensuite, il incombe au client d'en aviser les autorités de surveillance, de poursuite pénale ou de protection des données. Il informe le prestataire de la procédure prévue en toute transparence.

8.2 Sur demande, le prestataire prouve le respect des dispositions relatives à la protection des données et de l'accord ST par des moyens appropriés et fournit au client tous les renseignements requis. Le client peut contrôler le respect de ces obligations dans la mesure nécessaire. Si une inspection par l'autorité de surveillance, le client ou un auditeur mandaté par celui-ci, est nécessaire au cas par cas, celle-ci est réalisée, après avoir été annoncée de manière appropriée, aux horaires d'ouverture et en tenant compte des processus opérationnels du prestataire. Le prestataire peut conditionner l'inspection à une déclaration de confidentialité relative aux données d'autres clients et à la mise en place de mesures techniques et organisationnelles, dans la

mesure où cela ne porte pas atteinte à une obligation de confidentialité sanctionnée pénalement. Les concurrents du prestataire sont exclus de l'inspection dans tous les cas. Le client indemnise les dépenses occasionnées au prestataire de manière raisonnable.

9 Responsabilité

9.1 Vis-à-vis du client, le prestataire répond exclusivement des dommages résultant d'un traitement qu'il a effectué, pour lequel il a, par sa faute (a) ignoré des obligations légales ou contractuelles, (b) agi en ignorant les consignes données de manière licite par le client, ou (c) agi contrairement aux consignes données de manière licite par le client. Demeurent réservés les dommages causés par une faute légère, dont le prestataire ne répond pas.

9.2 Si le client est tenu d'indemniser la personne concernée, le recours contre le prestataire dans l'étendue visée au chiffre 9.1. ci-dessus lui demeure réservé. D'autres prétentions en responsabilité selon les lois en vigueur demeurent réservées.

10 Durée du contrat et effet du contrat

Sauf dispositions contraires dans le présent accord ST, la durée du présent accord ST est fondée sur la durée de l'accord de base. L'accord ST est valable au minimum tant que le prestataire traite des données personnelles du client, à moins que le présent accord ST ne soit remplacé par un autre contrat de sous-traitance valable qui soit conforme aux exigences légales.

11 Dispositions finales

11.1 Les droits et obligations découlant du rapport contractuel ne peuvent être ni cédés, ni transférés ni mis en gage sans l'accord de l'autre partie.

11.2 Dans les cas justifiés, le prestataire a le droit de modifier le présent accord ST. Dans ce cas, il est tenu d'annoncer préalablement les modifications. Sans opposition écrite dans un délai d'un mois suivant leur annonce, mais dans tous les cas lors de la première utilisation du produit ou du service du prestataire suivant l'annonce, les modifications sont réputées acceptées. En cas d'opposition, le client est libre de résilier l'accord de base avant la prise d'effet des modifications avec effet immédiat s'il ne parvient pas à s'entendre autrement avec le prestataire d'ici là.

11.3 Si une ou plusieurs dispositions du présent accord étaient nulles, leur nullité n'affecterait pas la validité des autres dispositions. Dans ce cas, les parties adapteront le contrat de manière à se rapprocher le plus possible du but visé par les dispositions nulles.

12 Droit applicable et for

Le présent accord ST est régi exclusivement par le droit suisse, exclusion faite des règles de conflits de lois et de la Convention des Nations Unies sur les contrats de vente internationale de marchandises. Le for exclusif est toujours le siège du client.

13 Signatures

Pour le prestataire:

Lieu et date: Frauenfeld, 30.08.2023

Emanuel Lorini
CEO

Mikael von Euw
CCO

zur Rose

Annexe 1

Afin de garantir la **confidentialité**, le prestataire doit prendre des mesures pour que:

a. les personnes autorisées aient accès uniquement aux données personnelles dont elles ont besoin pour accomplir leurs tâches (contrôle de l'accès);
   Mesures appropriées: connexion avec des comptes personnalisés, affectation et gestion des droits des utilisateurs en fonction du rôle

b. seules les personnes autorisées aient accès aux locaux et installations dans lesquels les données personnelles sont traitées (contrôle de l'accès);
   Mesures appropriées: sécurisation des portes avec un système de carte à puce pour les personnes autorisées, vidéosurveillance, réglementation applicable aux visiteurs consignée dans un procès-verbal, connexion avec des comptes personnalisés, affectation et gestion des droits des utilisateurs en fonction du rôle, utilisateurs admin personnels, authentification sécurisée via HIN

c. des personnes non autorisées ne puissent pas utiliser les systèmes de traitement de données automatisé au moyen de dispositifs de transfert de données (contrôle des utilisateurs).
   Mesures appropriées: connexion avec des comptes personnalisés, utilisation de mots de passe sûrs, blocage automatique de comptes, authentification multifactorielle pour l'accès VPN externe, procédures standard pour l'entrée / la sortie de collaborateurs, consignation des connexions des utilisateurs dans un procès-verbal.
   pare-feu, VPN avec authentification multifactorielle, cryptage des e-mails (HIN), échange de données sur des connexions cryptées, formations de sensibilisation et réalisation de campagnes de test de phishing, système de détection des mauvais comportements.

Afin de garantir la **disponibilité** et l'**intégrité**, le prestataire doit prendre des mesures pour que:

a. les personnes non autorisées ne puissent pas lire, copier, modifier, déplacer, effacer ou détruire des supports de données (contrôle des supports de données)
   Mesures appropriées: connexion avec des comptes personnalisés, utilisation de mots de passe sûrs, blocage automatique de comptes, authentification multifactorielle pour l'accès VPN externe, procédures standard pour l'entrée / la sortie de collaborateurs, consignation des connexions des utilisateurs dans un procès-verbal,
   pare-feu, VPN avec authentification multifactorielle, cryptage des e-mails (HIN), échange de données sur des connexions cryptées, formations de sensibilisation et réalisation de campagnes de test de phishing, système de détection des mauvais comportements.

b. les personnes non autorisées ne puissent pas enregistrer, lire, modifier, effacer ou détruire des données personnelles dans la mémoire (contrôle de la mémoire)
   Mesures appropriées: connexion avec des comptes personnalisés, affectation et gestion des droits des utilisateurs en fonction du rôle, utilisation de mots de passe sûrs, blocage automatique de comptes, authentification multifactorielle pour l'accès VPN externe, procédures standard pour l'entrée / la sortie de collaborateurs, consignation des connexions des utilisateurs dans un procès-verbal, pare-feu, VPN avec authentification multifactorielle.

c. les personnes non autorisées ne puissent pas lire, copier, modifier, effacer ou détruire des données personnelles lors de la communication de données personnelles ou du transport de supports de données (contrôle du transport)
   Mesures appropriées: Règles d'utilisation des supports de données mobiles

d. la disponibilité des données personnelles et l'accès aux données personnelles puissent être rapidement rétablis chez lui (rétablissement)
Mesures appropriées: sauvegarde plurigénérationnelle régulière

e. toutes les fonctions du système de traitement automatique des données soient disponibles (disponibilité), que les dysfonctionnements puissent être signalés (fiabilité) et que les données personnelles enregistrées ne puissent pas être endommagées par des dysfonctionnements du système (intégrité des données)
Mesures appropriées: redondances (Cm, systèmes, applications), procédure en cas d'incidents, monitoring

f. les systèmes d'exploitation et les logiciels d'application soient toujours à la pointe de la sécurité et que les failles critiques connues soient comblées (sécurité du système)
Mesures appropriées: gestion des failles et processus de gestion des patch

Afin de garantir la **traçabilité**, le prestataire doit prendre des mesures pour que:

a. il soit possible de vérifier quelles données personnelles ont été saisies ou modifiées, à quel moment et par quelle personne dans le système de traitement automatisé des données (contrôle de la saisie)
Mesures appropriées: logging applicatoire des activités

b. il soit possible de vérifier à qui des données personnelles sont communiquées au moyen de dispositifs de transmission de donnés (contrôle de la communication)
Mesures appropriées: non applicable

c. il soit possible d'identifier rapidement des violations de la sécurité des données (identification) et de prendre des mesures pour réduire ou éliminer les conséquences (élimination)
Mesures appropriées: système de détection des mauvais comportements et des intrus, afin de surveiller et de constater les abus, les activités douteuses, les utilisateurs non autorisés et les autres risques réels ou potentiels pour la sécurité. Procédure de Security Incident Response, processus de Business Continuity Management et de Desaster & Recovery.