zur Rose

# Vereinbarung für eine Auftragsdatenbearbeitung

zwischen

**den Nutzern von elektronischen Bestell- und Rezeptierungsservices und weiteren IT-Dienstleistungen von Zur Rose**
(«Kunde» / Verantwortlicher)

und

Zur Rose Suisse AG
Walzmühlestrasse 60
8500 Frauenfeld
(«Anbieter» / Auftragsbearbeiter)

## 1 Gegenstand und Geltungsbereich

**1.1** Diese Vereinbarung für eine Auftragsdatenbearbeitung («ADV») gilt dann, wenn der Auftragsbearbeiter im Auftrag des Kunden («Basis-Vereinbarung») Daten bearbeitet, insbesondere im Zusammenhang mit IT-Produkten und -Services. Diese konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien, die sich aus der in der Basis-Vereinbarung beschriebenen Auftragsdatenbearbeitung bzw. den Funktionen eines IT-Produktes ergeben.

**1.2** Sämtliche in dieser ADV beschriebenen Verpflichtungen finden Anwendung auf alle Tätigkeiten im Zusammenhang mit der Basis-Vereinbarung, bei denen der Anbieter, seine Mitarbeiter und von ihm beigezogene Dritte mit personenbezogenen Daten des Kunden («Personendaten») bearbeitet. Falls die Bestimmungen der ADV im Widerspruch zu den Bestimmungen der Basis-Vereinbarung stehen, gehen die Bestimmungen des ADV in jedem Fall vor.

**1.3** **Einschränkung des Geltungsbereichs**: Diese ADV erstreckt sich nicht auf die Bearbeitung von Kontaktdaten des Kunden bzw. seiner Mitarbeiter für die eigenen Zwecke des Anbieters und die Bearbeitung von Rezepten und andere Datenbearbeitungen durch Zur Rose Suisse AG in ihrer Funktion als Apotheke. Solche Bearbeitungen führt zur Rose Suisse AG selbständig als Verantwortliche durch.

**1.4** Der Anbieter bearbeitet Personendaten im Auftrag des Kunden gemäss der in der Basis-Vereinbarung vereinbarten Leistungen. Es können insbesondere folgende Personendaten betroffen sein:

- **Vorgenommene Datenbearbeitungen:** ergeben sich aus der Basis-Vereinbarung
- **Betroffene Datenkategorien:** insbesondere Personenstammdaten (z.B. Mitarbeiter, Patienten, Kunden); Gesundheitsdaten; Kontakt- und Kommunikationsdaten (Telefon, Email, IP-Adressen usw.); Vertragsdaten (z.B. Vertragsbeziehungen, Produktinteressen); Kundenhistorien; Abrechnungs- und Zahlungsdaten; Planungs- und Steuerungsdaten usw.
- **Besonders schützenswerte Personendaten:** insbesondere medizinische Patientendaten (z.B. Befunde, Medizinische Dokumentation, Diagnosen, Medikamente, Dokumente usw.); Daten über die Intimsphäre usw.
- **Kategorien von betroffenen Personen:** Patienten, Kunden, Interessenten, Mitarbeiter, Lieferanten und Geschäftspartner usw.

## 2 Verantwortlichkeiten und Gewährleistung

**2.1** Der Kunde ist im Rahmen dieser ADV und den erteilten Weisungen als «Verantwortlicher» für die Rechtmässigkeit der Datenbearbeitung und der Einhaltung von gesetzlichen Informationspflichten gegenüber Dritten verantwortlich.

**2.2** Der Anbieter gewährleistet, dass er seine Mitarbeiter und die von ihm beigezogenen Dritten zur Vertraulichkeit verpflichtet hat oder diese einer gesetzlich vorgeschriebenen Verschwiegenheitspflicht unterliegen. Zudem hat er diese Personen darauf hingewiesen, dass die Geheimhaltungsverpflichtung auch nach Beendigung ihrer Tätigkeit fortbesteht.

## 3 Weisungsbefugnis des Kunden

**3.1** Der Anbieter bearbeitet Personendaten nur im Rahmen des Vereinbarten und nach Weisung des Kunden. Davon ausgenommen sind Sachverhalte, in denen dem Anbieter eine Bearbeitung aus zwingenden rechtlichen Gründen auferlegt wird. Der Anbieter unterrichtet in derartigen Situationen den Kunden soweit zulässig vor Beginn der Bearbeitung über die entsprechenden rechtlichen Anforderungen.

**3.2** Dem Kunden steht im Rahmen dieser ADV ein Weisungsrecht über Art, Umfang und Verfahren der Datenbearbeitung zu, das er durch Einzelweisungen konkretisieren oder ergänzen kann. Der Anbieter informiert den Kunden, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstösst (wobei er keine entsprechende Prüfpflicht hat). Er kann die Umsetzung der Weisung solange aussetzen, bis sie vom Kunden unter Klärung der Haftung bestätigt oder abgeändert wurde.

## 4 Ort der Datenbearbeitung

Der Anbieter und die von ihm beigezogenen Dritten bearbeiten Personendaten in der Schweiz, einem Mitgliedsstaat der Europäischen Union (EU) oder einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR). Sofern der Anbieter einen Dritten ausserhalb dieses Gebiets beizieht, ist er für die Einhaltung der gesetzlichen Anforderungen hinsichtlich der Sicherstellung eines adäquaten Sicherheitsniveaus verantwortlich. Ziff. 7 bleibt vorbehalten.

## 5 Pflichten des Anbieters

**5.1** **Datenbearbeitung:** Der Anbieter verpflichtet sich, Personendaten und Bearbeitungsergebnisse nur im Rahmen der Weisungen des Kunden zu bearbeiten. Erhält der Anbieter eine behördliche Anordnung, Daten des Kunden herauszugeben, so hat er – sofern zulässig – den Kunden unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen.

**5.2** **Sicherheitsmassnahmen:** Der Anbieter gestaltet seine Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle dem Risiko angemessenen technischen und organisatorischen Massnahmen nach Stand der Technik, um die Vertraulichkeit, Verfügbarkeit und Integrität der Personendaten, die Nachvollziehbarkeit der Bearbeitung sowie die Belastbarkeit seiner diesbezüglichen Dienstleistungen sicherzustellen und beachtet dabei zumindest die in Anhang 1 festgehaltenen Sicherheitsmassnahmen. Er weist diese Massnahmen und deren Umsetzung auf Anfrage gegenüber dem Kunden und Aufsichtsbehörden nach.

**5.3** **Datenschutzfolgeabschätzung:** Falls der Kunde eine Datenschutzfolgeabschätzung vornehmen muss, liefert der Anbieter hinsichtlich der von ihm für den Kunden durchgeführten Bearbeitungen von Personendaten die für die Datenschutzfolgeabschätzung benötigten Fakten und technischen Informationen und unterstützt den Kunden entsprechend bei Konsultationen von Aufsichtsbehörden.

**5.4** **Unterstützungspflichten:** Der Anbieter unterstützt den Kunden bei der Einhaltung seiner gesetzlichen Pflichten hinsichtlich des Datenschutzes (z.B. Datensicherheitsmassnahmen, Meldungen von Verletzungen an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung betroffenen Person). Insbesondere unterrichtet der Anbieter den Kunden so rasch als möglich über alle

ihm bekannt gewordenen Verstösse gegen Vorschriften oder Weisungen hinsichtlich der Personendaten und trifft alle erforderlichen Massnahmen zur Sicherung und Minderung möglicher nachteiliger Folgen für die betroffenen Personen

**5.5** **Betroffenenrechte:** Der Anbieter ergreift die technischen und organisatorischen Massnahmen, damit der Kunde die Rechte der betroffenen Person gemäss den anwendbaren Datenschutzgesetzen insbesondere aber Information, Auskunft, Berichtigung und Löschung (bzw. Anonymisierung), Datenübertragbarkeit, Widerspruch sowie automatisierte Entscheidungsfindung im Einzelfall innert der gesetzlichen Frist erfüllen kann und überlässt dem Kunden alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Anbieter gerichtet, wird er den Antrag so rasch als möglich an den Kunden zur Bearbeitung weiterleiten.

**5.6** **Löschungs- und Herausgabepflicht:** Der Anbieter berichtigt, löscht (bzw. anonymisiert) oder sperrt Personendaten nur auf Anweisung des Kunden und stellt dabei datenschutzkonforme Prozesse sicher. Vorbehalten bleiben Auskunfts- und Herausgabepflichten. Bei Vertragsende oder auf Verlangen des Kunden hat der Anbieter, einzelne oder alle Bearbeitungsergebnisse und Unterlagen, die Personendaten enthalten, dem Kunden zu übergeben oder nach Absprache in dessen Auftrag zu vernichten, unter Vorbehalt einer vorübergehenden Speicherung von Personendaten in Backup- und Archivsystemen bis zur nächsten ordentlichen Löschung (für diese Personendaten gilt diese ADV weiter). Wenn der Anbieter die Daten in einem speziellen technischen Format verarbeitet, ist er gegen angemessene Aufwandentschädigung verpflichtet, die Daten entweder in diesem Format oder nach Wunsch des Kunden in einem anderen, gängigen Format herauszugeben, so dass diese möglichst ohne Verluste und unter Erhalt der Datenstruktur und Logik in eine neue Applikation überführt werden können

**5.7** **Protokollierung:** Werden besonders schützenswerte Personendaten in grossem Umfang automatisiert bearbeitet oder wird ein Profiling mit hohem Risiko durchgeführt, so weist der Kunde den Anbieter darauf hin, und der Anbieter muss zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten protokollieren. Die Protokollierung muss Aufschluss geben über die Identität der Person, die die Bearbeitung vorgenommen hat, die Art, das Datum und die Uhrzeit der Bearbeitung sowie gegebenenfalls die Identität der Empfängerin oder des Empfängers der Daten. Die Protokolle müssen während mindestens einem Jahr getrennt vom System, in welchem die Personendaten bearbeitet werden, aufbewahrt werden. Sie dürfen ausschliesslich den Organen und Personen zugänglich sein, denen die Überprüfung der Anwendung der Datenschutzvorschriften oder die Wahrung oder Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegt, und dürfen nur für diesen Zweck verwendet werden.

**5.8** **Kontrollpflicht**: Der Anbieter kontrolliert und dokumentiert die Erfüllung der vorgenannten Pflichten.

## 6 Wahrung des Berufsgeheimnisses

**6.1** Der Anbieter wird auch Daten bearbeiten oder darauf zugreifen können, die unter das Berufsgeheimnis im Sinne von Art. 321 StGB fallen und deren unbefugte Offenbarung nach StGB und DSG strafbar ist. Der Anbieter verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung

der ihm zugewiesenen Aufgaben erforderlich ist bzw. wie ihm der Kunde solche Daten übermittelt. Der Anbieter hat gegebenenfalls vom Zeugnisverweigerungsrecht gemäss Art. 171 StPO und vom Beschlagnahmeverbot gemäss Art. 262 StPO Gebrauch zu machen.

**6.2** Der Anbieter stellt sicher, dass alle Mitarbeiter und die von ihm beigezogenen Dritten sich schriftlich verpflichtet haben, die ihnen zugänglich gemachten Berufsgeheimnisse nicht unbefugt zu offenbaren und bestätigt haben, dass sie über die mögliche Strafbarkeit nach StGB und DSG belehrt wurden.

**6.3** Der Anbieter muss allfällige Unteranbieter sorgfältig auswählen und diese zur Geheimhaltung von dem Berufsgeheimnis unterliegenden Daten verpflichten, soweit sie darauf Zugriff haben. Weiter müssen solche Unteranbieter das eingesetzte Personal schriftlich zur Geheimhaltung verpflichten und über die Folgen einer Pflichtverletzung belehren. Dies gilt für alle weiteren Unteranbieter entsprechend.

## 7 Unterauftragsverhältnisse

**7.1** Soweit der Anbieter für die Bearbeitung von Personendaten Leistungen von Dritten in Anspruch nimmt, die in seinem Auftrag Personendaten bearbeiten («Unteranbieter»), listet der Anbieter deren Namen, Adressen und Aufgabenbereiche nachfolgend einzeln auf.

| Namen/Adresse | Aufgabenbereich | Ort der Datenbearbeitung |
|---|---|---|
| Clustertec AG, Baarmattstrasse 10, 6340 Baar | Applikationsentwicklung | Baar |
| BlueCare AG, Pflanzschulstrasse 3, 8400 Winterthur | Kunden-Onboarding, First-Level Support | Winterthur |

**7.2** Die allfällige Beauftragung anderer Unteranbieter ist dem Kunden schriftlich mitzuteilen. Ohne begründeten schriftlichen Widerspruch innert 30 Tagen gilt die Beauftragung als akzeptiert.

## 8 Informationspflichten und Auditrechte

**8.1** Der Anbieter informiert den Kunden im Fall einer Verletzung der Datensicherheit so rasch wie möglich. Er unterstützt den Kunden in der Aufarbeitung und stellt die ihm zugänglichen Unterlagen bereit. Es liegt anschliessend in der Verantwortung des Kunden, erforderliche Anzeigen an Datenschutz-, Strafverfolgungs- oder Aufsichtsbehörden zu veranlassen. Er informiert den Anbieter transparent über das geplante Vorgehen.

**8.2** Der Anbieter weist die Einhaltung der Datenschutzvorschriften und der ADV auf Anfrage mit geeigneten Mitteln nach und erteilt dem Kunden auf Anfrage alle erforderlichen Auskünfte. Der Kunde kann die Einhaltung dieser Verpflichtungen im erforderlichen Umfang kontrollieren. Sollte im Einzelfall eine Inspektion durch die Aufsichtsbehörde, den Kunden oder einen von diesem beauftragten Prüfer erforderlich sein, erfolgt diese nach angemessener Anmeldung zu den Geschäftszeiten und unter Rücksichtnahme auf den Betriebsablauf des Anbieters. Der Anbieter kann die Inspektion von einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Massnahmen abhängig machen soweit keine strafbewehrte Verschwiegenheitspflicht greift. Konkurrenten des Anbieters sind

von der Inspektion in jedem Fall ausgeschlossen. Der Kunde wird dem Anbieter die entstandenen Aufwände in angemessenem Umfang ersetzen.

## 9 Haftung

**9.1** Der Anbieter haftet dem Kunden ausschliesslich für Schäden, die auf einer von ihm durchgeführten Bearbeitung beruhen, bei der er schuldhaft (a) den gesetzlichen oder vertraglichen Verpflichtungen nicht nachgekommen ist, (b) unter Nichtbeachtung der rechtmässig erteilten Weisungen des Kunden handelte; oder (c) er gegen die rechtmässig erteilen Weisungen des Kunden gehandelt hat. Vorbehalten bleiben leichtfahrlässig verursachte Schäden, für die der Anbieter nicht haftet.

**9.2** Soweit der Kunde zum Schadenersatz gegenüber der betroffenen Person verpflichtet ist, bleibt ihm der Rückgriff auf den Anbieter im Umfang von Ziff. 9.1. vorstehend, vorbehalten. Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben vorbehalten.

## 10 Vertragsdauer und Vertragswirkung

Die Laufzeit dieser ADV richtet sich nach der Laufzeit der Basis-Vereinbarung, sofern sich aus den Bestimmungen dieser ADV nichts anderes ergibt. Die ADV gilt mindestens solange als der Anbieter Personendaten des Kunden bearbeitet, es sei denn diese ADV werde durch einen anderen gültigen Auftragsdatenbearbeitungsvertrag, der den gesetzlichen Anforderungen entspricht, abgelöst.

## 11 Schlussbestimmungen

**11.1** Rechte und Pflichten aus dem Vertragsverhältnis dürfen ohne Zustimmung der anderen Partei weder abgetreten, übertragen oder verpfändet werden.

**11.2** Dem Anbieter steht in begründeten Fällen das Recht zu, diese ADV zu ändern. Dabei obliegt es dem Anbieter, die Änderungen vorgängig bekannt zu geben. Ohne schriftlichen Widerspruch innert Monatsfrist nach Bekanntgabe, auf jeden Fall aber mit der ersten Nutzung der Produkte oder Services des Anbieters seit Bekanntgabe, gelten die Änderungen als genehmigt. Im Widerspruchsfall steht es dem Kunden frei, die Basis-Vereinbarung vor Inkrafttreten der Änderungen mit sofortiger Wirkung zu kündigen, falls der Kunde sich mit dem Anbieter bis zu jenem Zeitpunkt nicht anderweitig einigen kann.

**11.3** Sollten sich eine oder mehrere Bestimmungen dieses Vertrags als unwirksam erweisen, ist dadurch die Gültigkeit der übrigen Bestimmungen nicht betroffen. Die Parteien werden in einem solchen Fall den Vertrag so anpassen, dass der mit dem unwirksamen Teil angestrebte Zweck möglichst erreicht wird.

## 12 Anwendbares Recht und Gerichtsstand

Auf diese ADV ist ausschliesslich schweizerisches Recht unter Ausschluss des internationalen Kollisionsrechts sowie des Übereinkommens der Vereinigten Nationen über Verträge über den internationalen Warenkauf anwendbar. Ausschliesslicher Gerichtsstand ist stets am Sitz des Kunden.

## 13 Unterschriften

**Für den Anbieter:**

Ort und Datum: Frauenfeld, 30.08.2023

Emanuel Lorini
CEO

Mikael von Euw
CCO

zur Rose

## Anhang 1

Um die **Vertraulichkeit** zu gewährleisten, muss der Anbieter Massnahmen treffen, damit:

a. berechtigte Personen nur auf diejenigen Personendaten Zugriff haben, die sie zur Erfüllung ihrer Aufgaben benötigen (Zugriffskontrolle);
Geeignete Massnahmen: Login mit personalisierten Accounts, Rollenbasierte Zuordnung und Verwaltung von Benutzerberechtigungen

b. nur berechtigte Personen Zugang zu den Räumlichkeiten und Anlagen haben, in denen Personendaten bearbeitet werden (Zugangskontrolle);
Geeignete Massnahmen: Türsicherung mit Chipkarten-System für befugte Personen, Videoüberwachung, protokollierte Besucherregelung, Login mit personalisierten Accounts, Rollenbasierte Zuordnung und Verwaltung von Benutzerberechtigungen, persönliche Admin-Benutzer, sichere Authentifizierung über HIN

c. unbefugte Personen automatisierte Datenbearbeitungssysteme nicht mittels Einrichtungen zur Datenübertragung benutzen können (Benutzerkontrolle).
Geeignete Massnahmen: Login mit personalisierten Accounts, Einsatz sicherer Passwörter, Automatische Sperrung von Accounts, Multi-Faktor-Authentifizierung für externen VPN-Zugriff, Standard-Prozesse für Eintritt-/Austritt von Mitarbeitenden, Protokollierung der Benutzeranmeldungen.
Firewall, VPN mit Multifaktor-Authentifizierung, E-Mailverschlüsselung (HIN), Datenaustausch über verschlüsselte Verbindungen, Sensibilisierungs-Schulungen und Durchführung von Phishingtest-Kampagnen, System zur Erkennung von schadhaftem Verhalten.

Um **Verfügbarkeit** und **Integrität** zu gewährleisten, muss der Anbieter Massnahmen treffen, damit:

a. unbefugte Personen Datenträger nicht lesen, kopieren, verändern, verschieben, löschen oder vernichten können (Datenträgerkontrolle)
Geeignete Massnahmen: Login mit personalisierten Accounts, Einsatz sicherer Passwörter, Automatische Sperrung von Accounts, Multi-Faktor-Authentifizierung für externen VPN-Zugriff, Standard-Prozesse für Eintritt-/Austritt von Mitarbeitenden, Protokollierung der Benutzeranmeldungen,
Firewall, VPN mit Multifaktor-Authentifizierung, E-Mailverschlüsselung (HIN), Datenaustausch über verschlüsselte Verbindungen, Sensibilisierungs-Schulungen und Durchführung von Phishingtest-Kampagnen, System zur Erkennung von schadhaftem Verhalten.

b. unbefugte Personen Personendaten im Speicher nicht speichern, lesen, ändern, löschen oder vernichten können (Speicherkontrolle)
Geeignete Massnahmen: Login mit personalisierten Accounts, Rollenbasierte Zuordnung und Verwaltung von Benutzerberechtigungen, Einsatz sicherer Passwörter, Automatische Sperrung von Accounts, Multi-Faktor-Authentifizierung für externen VPN-Zugriff, Standard-Prozesse für Eintritt-/Austritt von Mitarbeitenden, Protokollierung der Benutzeranmeldungen, Firewall, VPN mit Multifaktor-Authentifizierung.

c. unbefugte Personen bei der Bekanntgabe von Personendaten oder beim Transport von Datenträgern Personendaten nicht lesen, kopieren, verändern, löschen oder vernichten können (Transportkontrolle)
Geeignete Massnahmen: Regeln für den Umgang mit mobilen Datenträgern

d. die Verfügbarkeit der Personendaten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können (Wiederherstellung)
Geeignete Massnahmen: regelmässige Mehrgenerationen-Backups

e. alle Funktionen des automatisierten Datenbearbeitungssystems zur Verfügung stehen (Verfügbarkeit), Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität)
Geeignete Massnahmen: Redundanzen (RZ, Systeme, Applikationen), Incident Prozess, Monitoring

f. Betriebssysteme und Anwendungssoftware stets auf dem neusten Sicherheitsstand gehalten und bekannte kritische Lücken geschlossen werden (Systemsicherheit)
Geeignete Massnahmen: Schwachstellenmanagement- und Patchmanagement-Prozess

Um die **Nachvollziehbarkeit** zu gewährleisten, muss der Anbieter Massnahmen treffen, damit:

a. überprüft werden kann, welche Personendaten zu welcher Zeit und von welcher Person im automatisierten Datenbearbeitungssystem eingegeben oder verändert werden (Eingabekontrolle)
Geeignete Massnahmen: Applikatorisches Logging der Aktivitäten

b. überprüft werden kann, wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekanntgegeben werden (Bekanntgabekontrolle)
Geeignete Massnahmen: nicht zutreffend

c. Verletzungen der Datensicherheit rasch erkannt (Erkennung) und Massnahmen zur Minderung oder Beseitigung der Folgen ergriffen werden können (Beseitigung)
Geeignete Massnahmen: System zur Erkennung von schadhaftem Verhalten und Eindringlingen, um Missbrauchsmuster, verdächtige Aktivitäten, unbefugte Nutzer und sonstige tatsächliche oder drohende Sicherheitsrisiken zu überwachen und festzustellen. Security Incident Response Prozess, Business Continuity Management- und Desaster & Recovery Prozesse.