Bestätigung der Auftragsverarbeitung (nachstehend 'Bestätigung' genannt)

HRM Systems AG
Technikumstrasse 82
8401 Winterthur
(nachstehend 'Auftragnehmer' genannt)

1 Gegenstand

HRM Systems AG bearbeitet im Auftrag des Kunden ('Auftraggeber') personenbezogene Daten von dessen Mitarbeitenden. Bei der Auslagerung von Datenverarbeitungsprozessen hat der Auftraggeber (Verantwortlicher) sich zu vergewissern, dass der Auftragsnehmer in der Lage ist, die Datensicherheit zu gewährleisten.

Diese Bestätigung zur Auftragsverarbeitung gewährleistet dem Auftraggeber die jederzeitige Einhaltung der geltenden Gesetze und Vorschriften über personenbezogene Daten, insbesondere des Schweizerischen Bundesgesetzes über den Datenschutz (DSG) und dessen Ausführungsverordnungen durch den Auftragnehmer.

Die effektiven Leistungen des Auftragsverhältnisses ergeben sich aus dem bestehenden Software- und Dienstleistungsvertrag (nachfolgend 'Hauptvertrag') zwischen Auftraggeber und Auftragnehmer.

2 Konkretisierung des Auftragsinhalts

2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber werden wie folgt beschrieben:

2.1.1 Art

Erheben, Erfassen, Organisieren, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten.

2.1.2 Zweck

Der Zweck der Datenverarbeitung ergibt sich aus dem Hauptvertrag. In diesem Rahmen kann der Auftragnehmer direkten oder indirekten Zugriff auf personenbezogene Daten des Auftraggebers haben.

Der Auftragnehmer verarbeitet personenbezogene Daten ausschliesslich im Auftrag und auf Weisung des Auftraggebers und nur für die Zwecke des Auftraggebers und die Vertragserfüllung. Die Parteien sind für die Einhaltung der gesetzlichen Bestimmungen der anwendbaren Datenschutzgesetze verantwortlich. Der Auftraggeber ist für die Rechtmässigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmässigkeit der Datenverarbeitung allein verantwortlich.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung (inklusive der Verarbeitung durch Unterauftragnehmer) findet in der Schweiz statt. Jede Verlagerung ausserhalb der Schweiz bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die Voraussetzungen der anwendbaren Datenschutzgesetze erfüllt sind.

2.2 Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten bilden folgende Datenarten:

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail, Tickets, Chat)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Anmeldedaten, personenbeziehbare oder personenbezogene Protokolldaten
- Alle anderen personenbezogenen Daten vom Auftraggeber im Zuge der Nutzung der Dienstleistungen übermittelt oder gespeichert werden.

2.3 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Mitarbeitende des Auftraggebers
- Weitere Ansprechpartner im Hinblick auf die Vertragserfüllung

3 Technisch-organisatorische Massnahmen

3.1 Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten erforderlichen technischen und organisatorischen Massnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Massnahmen Grundlage des Auftrags. Soweit die Prüfung des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

3.2 Der Auftragnehmer hat die Sicherheit der Verarbeitung zu gewährleisten. Er trifft angemessene organisatorische und technische Massnahmen zur Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und der Zweck der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen.

3.3 Die technischen und organisatorischen Massnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate, aber nicht weniger weit gehende Massnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Massnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4 Berichtigung, Einschränkung und Löschung von Daten

4.1 Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

4.2 Sofern vom Leistungsumfang umfasst, sind Löschkonzepte, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat sämtlichen gesetzlichen Pflichten des Auftragsverarbeiters nachzukommen; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- Der Auftragnehmer verpflichtet sich, sämtliche Informationen, Konzepte und Verfahren und insbesondere personenbezogene Daten des Auftraggebers geheim zu halten
- Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und vorgängig mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Dies gilt auch für andere für den Auftragnehmer tätige Personen. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschliesslich entsprechend der Weisung des Auftraggebers verarbeiten.
- Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Massnahmen gemäss Anlage 1.
- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- Die unverzügliche Information des Auftraggebers über jegliche Datenschutzverletzung oder vermutete Datenschutzverletzung, Kontrollhandlungen und Massnahmen der

Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

- Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- Der Auftragnehmer kontrolliert regelmässig die internen Prozesse sowie die technischen und organisatorischen Massnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts und den Vorgaben dieser Bestätigung erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Massnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieser Bestätigung.

6 Unterauftragsverhältnisse

6.1 Als Unterauftragsverhältnisse im Sinne dieser Bestätigung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen erbringt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmassnahmen zu ergreifen.

6.2 Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen, nachdem er diese sorgfältig ausgewählt und geprüft hat.
Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt.

6.3 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

Eine Weiter- oder Herausgabe von personenbezogenen Daten an Dritte ist, ohne vorherige schriftliche Zustimmung des Auftraggebers nicht zulässig.

6.4 Der Auftragnehmer prüft die Einhaltung der Pflichten durch die Unterbeauftragten. Das Ergebnis der Prüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen offenzulegen. Der Auftraggeber oder ein von ihm beauftragter Prüfer muss berechtigt sein, im Bedarfsfall selbst angemessene Überprüfungen und Inspektionen bei den Unterauftragnehmern durchzuführen.

6.5 Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers und des Hauptauftragnehmers. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7 Kontrollrechte des Auftraggebers

7.1 Der Auftraggeber hat das Recht, Überprüfungen beim Auftragnehmer durchzuführen oder durch im Einzelfall vom Auftraggeber benannte Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

7.2 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers als Auftragsverarbeiter überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Massnahmen nachzuweisen.

7.3 Der Nachweis solcher Massnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragte, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits (z.B. nach ISO-27001)

7.4 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen angemessenen Vergütungsanspruch geltend machen.

8 Unterstützung hinsichtlich Einhaltung der anwendbaren Datenschutzbestimmungen

8.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung datenschutzrechtlicher Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Massnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

8.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine angemessene Vergütung beanspruchen.

9 Weisungsbefugnis des Auftraggebers

9.1 Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mindestens Textform).

9.2 Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstosse gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

10 Löschung und Rückgabe von personenbezogenen Daten

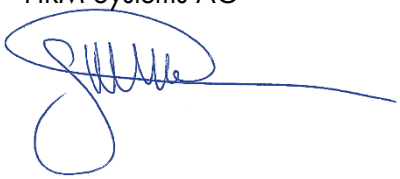
10.1 Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemässen Datenverarbeitung erforderlich sind sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

10.2 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber - spätestens mit Beendigung der Leistungsvereinbarung - hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auf Verlangen auszuhändigen oder nach dessen vorheriger Zustimmung datenschutzgerecht zu vernichten und dafür zu sorgen, dass dies auch seine Subauftragnehmer tun. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Antrag vorzulegen.

10.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemässen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Winterthur, den 15.06.2023

HRM Systems AG



Georg Hartmann
Geschäftsleiter

Anlage 1: technisch-organisatorische Massnahmen

1 Vertraulichkeit

- Zutrittskontrolle:
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B. Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen

- Zugangskontrolle:
  Keine unbefugte Systembenutzung, z.B. sichere Kennwörter, automatische Sperrmechanismen, zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern

- Zugriffskontrolle:
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B. Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen

- Trennungskontrolle:
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing

- Pseudonymisierung:
  Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen

2 Integrität

- Weitergabekontrolle:
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B. Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur

- Eingabekontrolle:
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B. Protokollierung, Dokumentenmanagement

3 Verfügbarkeit und Belastbarkeit

- Verfügbarkeitskontrolle:
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B. Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne

- Rasche Wiederherstellbarkeit

4 Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

- Datenschutz-Management

- Incident-Response-Management

- Datenschutzfreundliche Voreinstellungen

- Auftragskontrolle

Eine Auftragsdatenverarbeitung kann ohne entsprechende Weisung des Auftraggebers nicht stattfinden, z.B. eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.