Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 der Verordnung (EU) 2016/679 (DSGVO)

zwischen
Firma: _____
Anschrift: _____
Register-/USt-Nr.: _____
Vertreten durch: _____
(nachfolgend „Verantwortlicher“)

und

SANICURA d.o.o.
Ulica Andrije Hebranga 8, 10000 Zagreb, Kroatien
OIB 87611335623 · MBS 081712921 · USt-IdNr. HR87611335623
vertreten durch Martin Eckerstorfer, Geschäftsführer
handelnd unter der Marke „sigmacode.io“
Datenschutzkontakt: eckerstorfer@sanicura.com
(nachfolgend „sigmacode“ oder „Auftragsverarbeiter“)

einzeln „Partei“, gemeinsam „Parteien“.

> Hauptvertrag / Angebot vom _____ (der „Hauptvertrag“)

1. Gegenstand und Dauer

Dieser Auftragsverarbeitungsvertrag („AVV“) regelt die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen im Zusammenhang mit den Leistungen nach dem Hauptvertrag. Begriffe wie „personenbezogene Daten“, „Verarbeitung“, „Verletzung des Schutzes personenbezogener Daten“ und „Aufsichtsbehörde“ haben die Bedeutung, die ihnen in der DSGVO zukommt.

Dieser AVV gilt für die Laufzeit des Hauptvertrags und darüber hinaus, solange der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, insbesondere bis zur Löschung oder Rückgabe aller personenbezogenen Daten gemäß Ziffer 9.

2. Art und Zweck der Verarbeitung; Daten und betroffene Personen

Art und Zweck der Verarbeitung, die Kategorien personenbezogener Daten, die Kategorien betroffener Personen, die Dauer sowie der Ort der Verarbeitung sind in Anlage 1 festgelegt. Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur, soweit dies zur Erfüllung des Hauptvertrags erforderlich ist.

3. Weisungen des Verantwortlichen

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung in Drittländer –, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Der Hauptvertrag und dieser AVV stellen die ursprünglichen dokumentierten Weisungen des Verantwortlichen dar. Weitere Weisungen erfolgen in Textform (z. B. per E-Mail) und sind von beiden Parteien zu dokumentieren. Weisungen, die über den Leistungsumfang des Hauptvertrags hinausgehen, werden als Änderungswunsch behandelt.

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn eine Weisung seiner Auffassung nach gegen die DSGVO oder andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

4. Vertraulichkeit

Der Auftragsverarbeiter gewährleistet, dass sich alle zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Diese Verpflichtung besteht auch nach Beendigung ihrer Tätigkeit fort. Zugang zu personenbezogenen Daten wird nur gewährt, soweit dies für die Erfüllung des Hauptvertrags erforderlich ist.

5. Sicherheit der Verarbeitung

Der Auftragsverarbeiter trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen („TOM“) gemäß Anlage 2 unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Risiken für die Rechte und Freiheiten der betroffenen Personen.

Die TOM unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragsverarbeiter darf alternative adäquate Maßnahmen umsetzen, sofern das Schutzniveau der in Anlage 2 festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren und dem Verantwortlichen auf Anfrage mitzuteilen.

6. Unterauftragsverarbeiter

Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine schriftliche Genehmigung, Unterauftragsverarbeiter einzusetzen. Die bei Abschluss dieses AVV genehmigten bzw. je Projekt vor Beginn der Verarbeitung ergänzten Unterauftragsverarbeiter sind in Anlage 3 aufgeführt.

Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 30 Tage im Voraus in Textform über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters. Der Verantwortliche kann der Änderung innerhalb von 14 Tagen nach Zugang der Mitteilung aus berechtigten datenschutzrechtlichen Gründen widersprechen. In diesem Fall bemühen sich die Parteien nach Treu und Glauben um eine einvernehmliche Lösung. Kommt keine Lösung zustande, kann der Verantwortliche die von der Änderung betroffenen Leistungen zum Zeitpunkt des Wirksamwerdens der Änderung kündigen.

Setzt der Auftragsverarbeiter einen Unterauftragsverarbeiter ein, erlegt er diesem vertraglich dieselben Datenschutzpflichten auf, die in diesem AVV festgelegt sind, insbesondere hinreichende Garantien für geeignete TOM. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Unterauftragsverarbeiters.

Nebenleistungen, die der Auftragsverarbeiter ohne Zugriff auf personenbezogene Daten des Verantwortlichen in Anspruch nimmt (z. B. Telekommunikation, allgemeine Bürodienstleistungen), sind keine Unterauftragsverarbeitung im Sinne dieser Ziffer.

7. Unterstützung des Verantwortlichen

Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragsverarbeiter den Verantwortlichen

(a) bei der Erfüllung seiner Pflicht zur Beantwortung von Anträgen betroffener Personen auf Wahrnehmung ihrer Rechte nach Kapitel III DSGVO. Der Auftragsverarbeiter leitet unmittelbar an ihn gerichtete Anträge unverzüglich an den Verantwortlichen weiter und beantwortet diese nicht selbst, es sei denn, er wurde vom Verantwortlichen hierzu angewiesen;

(b) bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO, einschließlich der Sicherheit der Verarbeitung, der Meldung von Verletzungen des Schutzes personenbezogener Daten, Datenschutz-Folgenabschätzungen und der vorherigen Konsultation der Aufsichtsbehörde.

Unterstützungsleistungen, zu denen der Auftragsverarbeiter gesetzlich verpflichtet ist oder die auf einem eigenen Verstoß gegen diesen AVV beruhen, erbringt er unentgeltlich. Für darüber hinausgehende umfangreiche Unterstützung kann der Auftragsverarbeiter angemessene Kosten auf Basis der Sätze des Hauptvertrags berechnen, sofern er den Verantwortlichen hierauf vorab hingewiesen hat.

8. Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten, die personenbezogene Daten des Verantwortlichen betrifft, unverzüglich, spätestens jedoch innerhalb von 48 Stunden, nachdem sie ihm bekannt geworden ist.

Die Meldung enthält, soweit verfügbar, mindestens:

(a) eine Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze;

(b) den Namen und die Kontaktdaten einer Anlaufstelle für weitere Informationen;

(c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung;

(d) eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Können die Informationen nicht zur gleichen Zeit bereitgestellt werden, können sie ohne unangemessene weitere Verzögerung schrittweise zur Verfügung gestellt werden. Der Auftragsverarbeiter ergreift die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen und dokumentiert alle Verletzungen einschließlich der zugrunde liegenden Fakten, ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen.

9. Löschung und Rückgabe personenbezogener Daten

Nach Abschluss der Leistungen löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag verarbeiteten personenbezogenen Daten oder gibt sie an den Verantwortlichen zurück und löscht vorhandene Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung besteht.

Personenbezogene Daten in Datensicherungen werden im regulären Rotationszyklus der Backups gelöscht; bis dahin bleiben sie nach Maßgabe dieses AVV geschützt und werden nicht aktiv verarbeitet. Der Auftragsverarbeiter bestätigt die Löschung auf Verlangen schriftlich (Textform genügt).

10. Informationen und Kontrollen

Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO und diesem AVV niedergelegten Pflichten zur Verfügung.

Der Auftragsverarbeiter ermöglicht Überprüfungen einschließlich Inspektionen, die vom Verantwortlichen oder einem von diesem beauftragten, zur Verschwiegenheit verpflichteten Prüfer, der kein Wettbewerber des Auftragsverarbeiters ist, durchgeführt werden, und trägt dazu bei. Überprüfungen sind mit angemessener Frist (in der Regel 30 Tage) anzukündigen, während der üblichen Geschäftszeiten ohne unverhältnismäßige Störung des Betriebsablaufs durchzuführen und finden höchstens einmal pro Kalenderjahr statt, es sei denn, es liegt eine Verletzung des Schutzes personenbezogener Daten, ein begründeter Verdacht auf einen wesentlichen Verstoß gegen diesen AVV oder eine Anordnung einer Aufsichtsbehörde vor.

Der Auftragsverarbeiter kann zunächst geeignete Nachweise wie vorhandene Zertifizierungen, Prüfberichte oder ausgefüllte Fragebögen vorlegen, soweit diese zum Nachweis ausreichen. Jede Partei trägt ihre eigenen Kosten einer Überprüfung, es sei denn, die Überprüfung ergibt einen wesentlichen Verstoß des Auftragsverarbeiters gegen diesen AVV; in diesem Fall trägt der Auftragsverarbeiter die angemessenen Kosten der Überprüfung.

11. Internationale Datenübermittlungen

Der Auftragsverarbeiter übermittelt personenbezogene Daten – auch über Unterauftragsverarbeiter – nicht in ein Land außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums („Drittland“) oder an eine internationale Organisation, es sei denn, der Verantwortliche hat dies dokumentiert angewiesen oder genehmigt (auch durch Aufnahme des Empfängers in Anlage 3) und die Voraussetzungen des Kapitels V DSGVO sind erfüllt.

Übermittlungen sind insbesondere zulässig auf Grundlage

(a) eines Angemessenheitsbeschlusses der Europäischen Kommission nach Art. 45 DSGVO, einschließlich des EU-U.S. Data Privacy Framework für danach zertifizierte Empfänger; oder

(b) der Standardvertragsklauseln gemäß Durchführungsbeschluss (EU) 2021/914 der Kommission im jeweils passenden Modul, ergänzt um zusätzliche Maßnahmen, soweit diese nach einer Transfer-Folgenabschätzung (Transfer Impact Assessment) erforderlich sind.

12. Haftung

Die Haftung der Parteien gegenüber betroffenen Personen richtet sich nach Art. 82 DSGVO. Im Übrigen gelten für diesen AVV die Haftungsregelungen des Hauptvertrags, soweit zwingendes Recht nicht entgegensteht.

13. Laufzeit und Beendigung

Dieser AVV tritt mit Unterzeichnung durch beide Parteien in Kraft und endet mit Beendigung des Hauptvertrags. Die Pflichten aus diesem AVV gelten fort, solange der Auftragsverarbeiter personenbezogene Daten des Verantwortlichen besitzt. Eine gesonderte Kündigung dieses AVV ist nur zusammen mit dem Hauptvertrag bzw. den betroffenen Leistungen möglich.

14. Schlussbestimmungen

Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag geht dieser AVV in Bezug auf den Schutz personenbezogener Daten vor. Änderungen und Ergänzungen dieses AVV und seiner Anlagen bedürfen der Schrift- oder Textform; elektronische Signaturen (einschließlich qualifizierter und fortgeschrittener elektronischer Signaturen nach eIDAS) sowie der Austausch unterzeichneter Scans genügen.

Sollte eine Bestimmung dieses AVV unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt; an die Stelle der unwirksamen Bestimmung tritt eine wirksame Regelung, die dem Willen der Parteien und den Anforderungen der DSGVO am nächsten kommt.

Dieser AVV unterliegt dem auf den Hauptvertrag anwendbaren Recht; fehlt eine solche Rechtswahl, gilt das Recht der Republik Kroatien. Dieser AVV liegt in deutscher und englischer Sprache vor; im Zweifel gilt die englische Fassung.

Anlagen

Anlage 1 — Einzelheiten der Verarbeitung
Anlage 2 — Technische und organisatorische Maßnahmen
Anlage 3 — Unterauftragsverarbeiter

Für den Verantwortlichen (Kunde)	**Für den Auftragsverarbeiter (SANICURA d.o.o.)**
Ort, Datum	Ort, Datum
Name, Funktion	Name, Funktion
Unterschrift	Unterschrift

Anlage 1 — Einzelheiten der Verarbeitung

Je Projekt vor Beginn der Verarbeitung auszufüllen.

Gegenstand / Projekt	*z. B. Entwicklung und Betrieb der Webanwendung „…“*
Art der Verarbeitung	*z. B. Hosting, Entwicklung, Tests mit Produktivdaten, Support und Wartung, KI-Verarbeitung*
Zweck der Verarbeitung	*z. B. Bereitstellung der Plattform für die Kunden des Verantwortlichen*
Kategorien betroffener Personen	*z. B. Kunden, Beschäftigte, Endnutzer, Interessenten – zu ergänzen*
Kategorien personenbezogener Daten	*z. B. Kontaktdaten, Kontodaten, Nutzungs- und Protokolldaten, Kommunikationsinhalte*
Besondere Kategorien (Art. 9 DSGVO)	*keine, sofern hier nicht angegeben*
Dauer / Aufbewahrung	*Laufzeit des Hauptvertrags; Aufbewahrungsfristen nach Weisung des Verantwortlichen*
Ort der Verarbeitung	*z. B. EU/EWR; im Übrigen siehe Anlage 3*

Anlage 2 — Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter setzt die folgenden grundlegenden Maßnahmen gemäß Art. 32 DSGVO um. Projektspezifische Maßnahmen können unten ergänzt werden.

Verschlüsselung

- Transportverschlüsselung mit TLS 1.2 oder höher für alle Verbindungen, über die personenbezogene Daten übertragen werden.
- Verschlüsselung ruhender Daten durch die eingesetzten Hosting- und Cloud-Anbieter.
- Festplattenvollverschlüsselung auf allen Arbeitsgeräten.

Zugangs- und Zugriffskontrolle

- Multi-Faktor-Authentifizierung für alle Administrations-, Code-Hosting- und Cloud-Konten.
- Minimalprinzip (Least Privilege) und rollenbasierte Berechtigungen; Zugriff nur, soweit für die Aufgabe erforderlich.
- Ausschließlich persönliche Konten – keine geteilten Zugangsdaten; Speicherung von Zugangsdaten in einem Passwortmanager.
- Regelmäßige Überprüfung der Berechtigungen; Entzug bei Ende des Einsatzes bzw. Offboarding.

Trennung

- Getrennte Umgebungen für Entwicklung, Staging und Produktion.
- Produktivdaten in Entwicklung oder Tests nur mit Zustimmung des Verantwortlichen; bevorzugt pseudonymisierte oder anonymisierte Testdaten.

Protokollierung und Überwachung

- Protokollierung von Zugriffen und administrativen Aktionen in den Audit-Logs der Anbieter, soweit verfügbar.
- Anwendungsprotokolle mit möglichst wenigen personenbezogenen Daten.
- Fehler-Monitoring so konfiguriert, dass personenbezogene Daten entfernt werden.

Verfügbarkeit und Belastbarkeit

- Datensicherungen der Daten des Verantwortlichen je Projekt beim Hosting-Anbieter; Wiederherstellung getestet.
- Infrastruktur als Code, soweit anwendbar, für eine reproduzierbare Wiederherstellung.

Sichere Entwicklung

- Code-Review für jede Änderung vor dem Deployment.
- Prüfung von Abhängigkeiten und Schwachstellen.
- Secrets in Secret-Managern, niemals in Quellcode-Repositories.
- Automatisierte Tests in der Continuous Integration; dem Projekt angemessene Sicherheitstests.

Datenminimierung und KI

- Es werden nur die für den jeweiligen Zweck erforderlichen personenbezogenen Daten verarbeitet.
- Bei KI-Funktionen: kein Training von Modellen mit Daten des Verantwortlichen; Auswahl des KI-Anbieters je Projekt, möglichst mit EU-Region; Entfernung personenbezogener Daten, soweit möglich.

Ort des Hostings

- Hosting in der EU/im EWR, soweit möglich; andernfalls gemäß Anlage 3 mit geeigneten Garantien für die Übermittlung.

Vorfallmanagement

- Dokumentierter Prozess zur Reaktion auf Sicherheitsvorfälle; Meldung von Datenschutzverletzungen an den Verantwortlichen innerhalb von 48 Stunden.

Personal

- Schriftliche Verpflichtung zur Vertraulichkeit; regelmäßige Sensibilisierung für Informationssicherheit.
- Arbeitsgeräte mit automatischer Bildschirmsperre und aktuellen Betriebssystem- und Sicherheitsupdates.

Löschung

- Sichere Löschung personenbezogener Daten bei Ende des Auftrags gemäß Ziffer 9.

Projektspezifische zusätzliche Maßnahmen:

Anlage 3 — Unterauftragsverarbeiter

Der Verantwortliche genehmigt die folgenden Unterauftragsverarbeiter. Die Liste wird je Projekt vor Beginn der Verarbeitung vervollständigt.

Unterauftragsverarbeiter (Name, Anschrift)	Leistung / Verarbeitungstätigkeit	Ort der Verarbeitung	Übermittlungsgrundlage (falls außerhalb EU/EWR)

Änderungen dieser Liste richten sich nach Ziffer 6: Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 30 Tage vor der Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters in Textform; der Verantwortliche kann innerhalb von 14 Tagen nach Zugang der Mitteilung aus berechtigten datenschutzrechtlichen Gründen widersprechen.