Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO

für SMART-Pedigree

Version: 1.0 **Stand:** 30.10.2026 **Hauptvertrag:** Lizenzvertrag der jeweiligen Bestellung oder Angebotsannahme

zwischen dem jeweiligen Lizenznehmer als Verantwortlichem und der PiehBerz IT-Solutions UG (haftungsbeschränkt), Bahnhofstraße 53, 64409 Messel, als Auftragsverarbeiter

Diese Vereinbarung zur Auftragsverarbeitung („AVV“) wird bei Abschluss des Lizenzvertrags mit dem jeweiligen Lizenznehmer als Verantwortlichem und der PiehBerz IT-Solutions UG (haftungsbeschränkt) als Auftragsverarbeiter geschlossen. Sie konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien für die in dieser AVV beschriebenen Verarbeitungsvorgänge. Der Lizenzvertrag der jeweiligen Bestellung oder Angebotsannahme ist der Hauptvertrag im Sinne dieser AVV. Die Anlagen 1 bis 3 sind Bestandteil dieser AVV.

§ 1 Vertragsschluss und Einbeziehung

(1) Im Online-Shop wird diese AVV gemeinsam mit den Allgemeinen Geschäfts- und Lizenzbedingungen (AGB/EULA) ausdrücklich akzeptiert. Der vollständige Text der AGB/EULA und dieser AVV ist vor Abgabe der Bestellung abrufbar und speicherbar. Die gemeinsame Akzeptanz erfolgt im Rahmen der Bestellung.

(2) Bei einem individuellen Angebot wird diese AVV als Anlage zum Angebot bereitgestellt. Mit der Annahme des Angebots wird zugleich diese AVV geschlossen.

(3) Der vollständige Vertragstext dieser AVV wird dem Lizenznehmer nach Vertragsschluss per E-Mail an die im Lizenzvertrag hinterlegte Kontaktadresse übermittelt. Die elektronische Übermittlung dient zugleich der Dokumentation des Vertragsschlusses.

(4) Diese AVV gilt nur für Einrichtungen mit einem aktiven Lizenzvertrag. Einrichtungen ohne aktive Lizenz, insbesondere Einrichtungen in einer Testphase, verwenden ausschließlich den hierfür vorgesehenen isolierten Supportweg ohne AVV. Über diesen isolierten Supportweg dürfen keine Patienten-, Gesundheits- oder genetischen Daten übermittelt werden.

§ 2 Gegenstand und Geltungsbereich

(1) Diese AVV regelt die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen im Rahmen von IT-Support, Fehleranalyse, Fehlerbehebung, Bug-Reporting und technischer Kommunikation über das Ticketsystem Zammad für SMART-Pedigree.

(2) Erfasst sind insbesondere Supporttickets, Fehlermeldungen, technische Kommunikation, die Dokumentation des jeweiligen Supportfalls und eine vom Verantwortlichen freiwillig übermittelte Sicherheitsprotokolldatei.

(3) Die lokale Verarbeitung von Patienten- und Gesundheitsdaten in SMART-Pedigree auf den Systemen des Verantwortlichen oder in dessen eigener Infrastruktur ist nicht Gegenstand dieser AVV. Für diese Verarbeitung bleibt der Verantwortliche datenschutzrechtlich zuständig und verantwortlich.

(4) Der Web- bzw. PDF-Fragebogen ist nicht Gegenstand dieser AVV. Die Eingaben des Webfragebogens werden clientseitig im Browser der ausfüllenden Person verarbeitet und nicht an den Auftragsverarbeiter übertragen.

(5) Diese AVV begründet keine Verpflichtung zur Übermittlung personenbezogener Daten. Der Verantwortliche übermittelt nur solche Daten, die für den konkreten Supportfall erforderlich sind.

§ 3 Dauer, Art und Zweck der Verarbeitung

(1) Die Verarbeitung beginnt mit dem Abschluss dieser AVV und erfolgt während der Laufzeit des Hauptvertrags, soweit der Verantwortliche personenbezogene Daten im Rahmen eines Supportfalls übermittelt oder zur Bearbeitung bereitstellt.

(2) Nach Beendigung des Hauptvertrags besteht diese AVV nur fort, soweit dies für die Rückgabe, Löschung, Nachweisführung oder eine gesetzlich zulässige Aufbewahrung erforderlich ist.

(3) Die Verarbeitung dient ausschließlich der Bearbeitung von Supporttickets, der Fehleranalyse, der Fehlerbehebung, dem Bug-Reporting, der technischen Kommunikation und der Dokumentation des jeweiligen Supportfalls.

(4) Zulässige Verarbeitungshandlungen sind das Erheben, Empfangen, Speichern, Ordnen, Auslesen, Abgleichen, Übermitteln innerhalb des Supportprozesses, Einschränken und Löschen, jeweils soweit dies für den konkreten Supportfall erforderlich ist.

(5) Eine Nutzung zu eigenen Zwecken des Auftragsverarbeiters, insbesondere zu Werbung, Profilbildung, Training von KI-Modellen oder einer allgemeinen Auswertung von Ticketinhalten, ist ausgeschlossen.

§ 4 Datenarten und Kategorien betroffener Personen

(1) Verarbeitet werden können insbesondere Namen, geschäftliche Kontaktdaten, Ticketinhalte, Kommunikationsdaten, technische Angaben, Fehlermeldungen, Screenshots, Logdateien und gegebenenfalls die vom Verantwortlichen freiwillig übermittelte Sicherheitsprotokolldatei.

(2) Das Sicherheitsprotokoll enthält nach dem vorgesehenen technischen Aufbau keine Patientendaten, Dateinamen, Lizenzschlüssel oder Hardwarekennungen. Jeder Eintrag enthält Datum und Uhrzeit. Das Protokoll liegt im Datenordner von SMART-Pedigree auf den Systemen der Einrichtung, je nach Installation im Programmordner, in einem von der IT festgelegten Ordner oder im Benutzerprofil. Es wird nur freiwillig im Rahmen eines Supportfalls übermittelt.

(3) Gesundheitsdaten und genetische Daten dürfen grundsätzlich nicht über den Supportweg übermittelt werden. Übermittelt der Verantwortliche solche Daten trotz dieses Verbots proaktiv in einem Supportticket oder Anhang und besteht für den Verantwortlichen eine wirksame AVV, werden sie im Rahmen des konkreten Supportfalls verarbeitet und unterliegen den Schutzmaßnahmen dieser AVV.

(4) Betroffene Personen sind Beschäftigte und Ansprechpartner des Verantwortlichen sowie mittelbar Patienten, soweit sie entgegen der vorgesehenen Datenminimierung in Ticketinhalten oder Anhängen genannt werden.

(5) Der Verantwortliche stellt sicher, dass nur die für den Supportfall erforderlichen Daten übermittelt werden. Patienten-, Gesundheits- und genetische Daten sowie nicht erforderliche Namen, Dateinamen, Inhalte und Anhänge sind vor der Übermittlung möglichst zu entfernen, zu anonymisieren oder zu schwärzen.

§ 5 Weisungen und Verantwortlichkeiten

(1) Der Verantwortliche entscheidet über die Zwecke und Mittel der Verarbeitung, soweit diese nicht durch den Gegenstand des Hauptvertrags und diese AVV festgelegt sind, und bleibt Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO.

(2) Der Auftragsverarbeiter ist Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO, soweit er personenbezogene Daten im Supportfall verarbeitet. Er verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, sofern nicht eine gesetzliche Verpflichtung zur Verarbeitung besteht.

(3) Weisungen werden durch den Verantwortlichen oder eine von ihm hierzu autorisierte Person über die vereinbarten Support- oder Vertragskanäle erteilt. Weisungen können insbesondere die Bereitstellung, Einschränkung, Berichtigung, Rückgabe oder Löschung von Daten betreffen.

(4) Mündliche Weisungen sind unverzüglich in Textform zu bestätigen. Der Auftragsverarbeiter dokumentiert Weisungen, soweit dies für die Nachvollziehbarkeit des Supportfalls erforderlich ist.

(5) Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, informiert er den Verantwortlichen unverzüglich. Bis zur Bestätigung oder Änderung der Weisung darf der Auftragsverarbeiter die betroffene Verarbeitung aussetzen, soweit dies technisch und organisatorisch möglich ist und keine zwingende gesetzliche Pflicht entgegensteht.

(6) Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung, die Erfüllung der Informationspflichten, die Auswahl der zu übermittelnden Daten und die Wahrung der Rechte betroffener Personen verantwortlich.

(7) Der Verantwortliche weist die für den Support zuständigen Personen darauf hin, personenbezogene Daten und insbesondere Gesundheits- oder genetische Daten nur über den vorgesehenen Supportweg und bei bestehender AVV zu übermitteln.

§ 6 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur im Rahmen dieser AVV, des Hauptvertrags und dokumentierter Weisungen.

(2) Der Auftragsverarbeiter stellt sicher, dass die zur Verarbeitung befugten Personen personenbezogene Daten nur auf Weisung des Verantwortlichen verarbeiten, soweit sie nicht gesetzlich zur Verarbeitung verpflichtet sind.

(3) Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen nach Art. 32 DSGVO und hält die in Anlage 2 beschriebenen Maßnahmen aufrecht, soweit sie für den jeweiligen Verarbeitungsvorgang erforderlich sind.

(4) Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Maßgabe der §§ 10 und 11 bei der Erfüllung seiner Pflichten nach der DSGVO.

(5) Der Auftragsverarbeiter führt ein Verzeichnis der Verarbeitungstätigkeiten, soweit die gesetzlichen Voraussetzungen hierfür erfüllt sind, und stellt dem Verantwortlichen die für dessen Nachweise erforderlichen Informationen zur Verfügung.

(6) Der Auftragsverarbeiter informiert den Verantwortlichen über wesentliche Änderungen der für die Verarbeitung eingesetzten technischen und organisatorischen Maßnahmen, soweit diese die Sicherheit oder den Umfang der Verarbeitung berühren.

(7) Der Auftragsverarbeiter verwendet personenbezogene Daten nicht für eigene Zwecke, insbesondere nicht für Werbung, Produktprofile, Profilbildung, Training von KI-Modellen oder eine allgemeine Auswertung von Ticketinhalten.

(8) Der Auftragsverarbeiter hält die gesetzlichen Anforderungen an die Verarbeitung besonderer Kategorien personenbezogener Daten ein, soweit solche Daten entgegen der vorgesehenen Datenminimierung übermittelt werden.

§ 7 Vertraulichkeit und Zugriff

(1) Der Auftragsverarbeiter verpflichtet die mit der Verarbeitung befassten Personen zur Vertraulichkeit oder unterwirft sie einer angemessenen gesetzlichen Verschwiegenheitspflicht. Die Verpflichtung besteht auch nach Beendigung ihrer Tätigkeit fort.

(2) Zugriff auf personenbezogene Daten erhalten ausschließlich autorisierte Personen, die ihn für die Bearbeitung eines aktiven Supportfalls benötigen.

(3) Als autorisierte Personen für Administration und Support sind Daniel Pieh und Florian Berz vorgesehen. Änderungen des autorisierten Personenkreises werden nach dem Berechtigungskonzept dokumentiert.

(4) Die Administration und der Support erfolgen ausschließlich aus Deutschland. Ein Zugriff aus Drittstaaten ist nicht vorgesehen.

(5) Kunden mit bestehender AVV werden im Ticketsystem unter einer eigenen Organisation geführt. Sie erhalten nur Zugriff auf die Tickets ihrer eigenen Organisation.

(6) Die Anmeldung ist nur mit Zwei-Faktor-Authentifizierung möglich. Änderungen an Tickets werden im Ticketverlauf protokolliert. Ein Protokollieren des bloßen Ansehens von Tickets wird nicht zugesagt.

§ 8 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter gewährleistet ein dem Risiko angemessenes Schutzniveau nach Art. 32 DSGVO. Die konkreten Maßnahmen sind in Anlage 2 beschrieben.

(2) Die Maßnahmen umfassen insbesondere Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit, Wiederherstellbarkeit, Zugriffskontrolle, logische Mandantentrennung, Übertragungsverschlüsselung, Datensicherung und regelmäßige Überprüfung.

(3) Der Auftragsverarbeiter darf die Maßnahmen weiterentwickeln, wenn das vereinbarte Schutzniveau nicht unterschritten wird und die gesetzlichen Anforderungen eingehalten werden.

(4) Änderungen, die das Schutzniveau wesentlich vermindern könnten, bedürfen einer vorherigen Information des Verantwortlichen und einer angemessenen Bewertung.

(5) Die technischen und organisatorischen Maßnahmen dieser AVV betreffen ausschließlich die konkrete Support-Auftragsverarbeitung. Sie ersetzen keine Vorgaben zur lokalen Infrastruktur des Verantwortlichen.

§ 9 Unterauftragsverarbeiter

(1) Der Verantwortliche genehmigt die in Anlage 3 aufgeführten Unterauftragsverarbeiter im Rahmen der dort beschriebenen Leistungen und Standorte.

(2) Der Auftragsverarbeiter darf weitere Unterauftragsverarbeiter nur auf Grundlage einer allgemeinen Genehmigung des Verantwortlichen einsetzen. Er informiert den Verantwortlichen vorab in Textform über jede beabsichtigte Hinzunahme oder Ersetzung und gibt ihm eine angemessene Einspruchsmöglichkeit.

(3) Der Einspruch muss innerhalb einer angemessenen Frist erfolgen und auf datenschutzrechtlich oder sicherheitsbezogen nachvollziehbare Gründe gestützt sein. Bei einem berechtigten Widerspruch suchen die Parteien eine zumutbare Lösung, etwa die Beendigung der betroffenen Teilverarbeitung oder den Einsatz eines geeigneten alternativen Dienstes.

(4) Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter durch Vertrag in gleicher Weise, wie er durch diese AVV verpflichtet ist, insbesondere zu geeigneten technischen und organisatorischen Maßnahmen sowie zu den Unterstützungs- und Kontrollpflichten.

(5) Der Auftragsverarbeiter bleibt gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Unterauftragsverarbeiters verantwortlich.

§ 10 Unterstützung bei Betroffenenrechten

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen durch geeignete technische und organisatorische Maßnahmen dabei, Anträge betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit oder Widerspruch nach den Art. 15 bis 22 DSGVO fristgerecht zu bearbeiten.

(2) Geht ein Antrag direkt beim Auftragsverarbeiter ein, leitet er ihn unverzüglich an den Verantwortlichen weiter und beantwortet ihn nicht eigenständig, sofern keine Weisung oder gesetzliche Verpflichtung hierzu besteht.

(3) Der Auftragsverarbeiter sucht die betroffenen Daten nach den vom Verantwortlichen bereitgestellten Angaben und stellt sie in einem angemessenen, gängigen Format bereit, soweit dies zur Bearbeitung des Antrags erforderlich ist.

(4) Der Verantwortliche stellt sicher, dass die zur Identifizierung erforderlichen Angaben rechtmäßig übermittelt werden und keine Rechte anderer Personen verletzt werden.

(5) Die Unterstützung erfolgt unverzüglich und unter Berücksichtigung der gesetzlichen Fristen. Erforderliche Nachfragen werden ohne unangemessene Verzögerung gestellt.

§ 11 Unterstützung bei Datenschutzpflichten und Datenschutzverletzungen

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm verfügbaren Informationen bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO.

(2) Die Unterstützung umfasst insbesondere Informationen zur Sicherheit der Verarbeitung, zur Meldung und Bewertung von Datenschutzverletzungen, zur Datenschutz-Folgenabschätzung sowie gegebenenfalls zur vorherigen Konsultation der Aufsichtsbehörde.

(3) Der Auftragsverarbeiter meldet dem Verantwortlichen eine Datenschutzverletzung unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis. Die Meldung enthält, soweit bekannt, Art und Zeitpunkt des Vorfalls, betroffene Daten und Personengruppen, mögliche Folgen sowie ergriffene oder vorgeschlagene Abhilfemaßnahmen.

(4) Ist eine vollständige Meldung innerhalb von 24 Stunden nicht möglich, werden die verfügbaren Informationen zunächst übermittelt und anschließend ohne unangemessene Verzögerung ergänzt.

(5) Der Auftragsverarbeiter dokumentiert Datenschutzverletzungen und die hierzu ergriffenen Maßnahmen, soweit dies gesetzlich erforderlich oder zur Unterstützung des Verantwortlichen notwendig ist.

(6) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über behördliche Anfragen oder sonstige Maßnahmen, die sich unmittelbar auf die im Auftrag verarbeiteten Daten beziehen, soweit dies gesetzlich zulässig ist.

(7) Der Auftragsverarbeiter übermittelt Behörden oder sonstigen Dritten keine personenbezogenen Daten aus dem Supportprozess, außer auf dokumentierte Weisung, aufgrund einer gesetzlichen Verpflichtung oder zur Abwehr einer gegen ihn gerichteten Rechtsforderung. Soweit gesetzlich zulässig, informiert er den Verantwortlichen vor einer solchen Übermittlung.

(8) Die Unterstützungspflichten dieses § 11 gelten unbeschadet zwingender gesetzlicher Pflichten und Rechte.

§ 12 Sicherheitsmeldungen und Datenminimierung

(1) Der Verantwortliche übermittelt an den Auftragsverarbeiter nur solche personenbezogenen Daten, die für den konkreten Supportfall erforderlich sind.

(2) Vor der Übermittlung sind Patienten-, Gesundheits- und genetische Daten sowie nicht erforderliche Namen, Dateinamen, Inhalte und Anhänge möglichst zu entfernen, zu schwärzen oder zu anonymisieren.

(3) Sicherheitsmeldungen werden in einer eigenen Gruppe des Ticketsystems verarbeitet. Sie werden organisatorisch und technisch von den übrigen Supportprozessen getrennt behandelt.

(4) Sicherheitsmeldungen werden zur Prüfung, Bewertung und Behebung gemeldeter Risiken sowie zur Erfüllung gesetzlicher Melde-, Dokumentations- und Abhilfepflichten verarbeitet.

(5) Anfragen ohne bestehende AVV werden in einem technisch und organisatorisch getrennten, isolierten Supportprozess mit restriktiven Zugriffsrechten verarbeitet. Ein automatisierter Hinweis untersagt die Übermittlung von Patienten-, Gesundheits- und genetischen Daten. Diese isolierten

Datensätze werden spätestens sechs Monate nach Eingang gelöscht, sofern keine Sicherheitsmeldung vorliegt.

(6) Für Sicherheitsmeldungen gilt eine Speicherfrist von drei Jahren zum Jahresende nach Abschluss der Bearbeitung. Eine längere Speicherung erfolgt nur, soweit gesetzliche Dokumentationspflichten oder die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dies erfordern.

(7) Sicherheitsmeldungen dürfen nicht zu Werbung, Profilbildung, Training von KI-Modellen oder einer sonstigen Ausweitung des Verarbeitungszwecks verwendet werden.

§ 13 Löschung und Rückgabe

(1) Der Verantwortliche entscheidet, ob die im Auftrag verarbeiteten personenbezogenen Daten nach Ende des Hauptvertrags zurückgegeben oder gelöscht werden. Die Weisung ist in Textform zu erteilen.

(2) Der Auftragsverarbeiter löscht oder gibt die Daten nach Weisung des Verantwortlichen zurück, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht. Die Wahl umfasst auch die Löschung oder Rückgabe vorhandener Kopien, soweit gesetzlich zulässig.

(3) Supporttickets samt Inhalten und Anhängen werden spätestens drei Jahre nach Ende des Kalenderjahres des finalen Abschlusses gelöscht. Für Sicherheitsmeldungen gilt die Frist nach § 12 Abs. 6.

(4) Die maximale Vorhaltezeit von Backups beträgt sechs Monate. Nach Ablauf dieser Frist werden die betreffenden Backups gelöscht oder überschrieben, soweit keine gesetzliche Aufbewahrung oder ein dokumentierter Sicherheits- oder Wiederherstellungszweck entgegensteht.

(5) Eine isolierte Supportanfrage ohne bestehende AVV wird spätestens sechs Monate nach Eingang gelöscht, sofern sie nicht zugleich eine Sicherheitsmeldung ist oder eine längere Aufbewahrung gesetzlich erforderlich ist.

(6) Nach Beendigung der Aufbewahrungsfrist werden Daten gelöscht oder, sofern eine Löschung technisch nicht möglich oder unverhältnismäßig wäre, wirksam anonymisiert. Die Anonymisierung muss eine Zuordnung zu einer Person mit vertretbarem Aufwand ausschließen.

(7) Dokumentations- und Nachweisdaten dürfen nur so lange aufbewahrt werden, wie dies gesetzlich erforderlich oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen notwendig ist. Danach sind sie zu löschen oder zu anonymisieren.

(8) Der Auftragsverarbeiter bestätigt dem Verantwortlichen die Durchführung einer angeordneten Löschung oder Rückgabe auf Verlangen in geeigneter Form.

§ 14 Nachweise und Kontrollen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten nach Art. 28 DSGVO und dieser AVV erforderlich sind.

(2) Hierzu gehören insbesondere angemessene Beschreibungen der technischen und organisatorischen Maßnahmen, Nachweise über die Verpflichtung zur Vertraulichkeit, Informationen zu Unterauftragsverarbeitern, Löschkonzepte, Sicherheitskonzepte und verfügbare Prüfberichte, soweit vorhanden.

(3) Der Verantwortliche ist berechtigt, die Einhaltung dieser AVV durch angemessene Kontrollen einschließlich Inspektionen zu überprüfen oder durch einen zur Vertraulichkeit verpflichteten Prüfer überprüfen zu lassen.

(4) Regelkontrollen sind mit angemessener Frist anzukündigen und so durchzuführen, dass der Geschäftsbetrieb und die Sicherheit anderer Kunden nicht unangemessen beeinträchtigt werden.

(5) Bei konkreten Anhaltspunkten für eine Verletzung dieser AVV, nach einer Datenschutzverletzung oder auf behördliche Anforderung sind Sonderkontrollen ohne unangemessene Verzögerung zu ermöglichen. Die berechtigten Interessen des Auftragsverarbeiters und anderer Verantwortlicher bleiben zu berücksichtigen.

(6) Der Verantwortliche und von ihm beauftragte Prüfer dürfen nur Informationen einsehen, die für die Prüfung der Auftragsverarbeitung erforderlich sind. Geschäftsgeheimnisse und Daten anderer Kunden sind zu schützen.

(7) Soweit Nachweise oder Kontrollen gesetzlich oder vertraglich ohnehin vorgesehen sind, entstehen hierfür keine gesonderten Kosten. Zusätzliche, vom Verantwortlichen veranlasste Sonderleistungen werden nur nach vorheriger Vereinbarung, transparent und angemessen nach dem tatsächlich erforderlichen Aufwand vergütet, soweit dies gesetzlich zulässig ist.

(8) Zwingende gesetzliche Kontroll- und Nachweisrechte des Verantwortlichen oder einer Aufsichtsbehörde werden durch diese Regelungen nicht abbedungen.

§ 15 Drittlandübermittlungen

(1) Die Verarbeitung durch den Auftragsverarbeiter und STRATO erfolgt ausschließlich in Deutschland. Ein Fernzugriff aus Drittstaaten ist nicht vorgesehen.

(2) Cloudflare, Inc. wird ausschließlich für den Einsatz von Turnstile auf der Website und auf Anmeldeformularen eingesetzt. Cloudflare wird nicht für das Ticketsystem eingesetzt und erhält keinen Zugriff auf Supporttickets oder die darin enthaltenen Daten.

(3) Soweit der Einsatz von Cloudflare einen Drittlandbezug oder einen Drittlandzugriff begründet, erfolgt er nur im konkret erforderlichen Umfang und auf Grundlage einer im konkreten Dienst tatsächlich anwendbaren Rechtsgrundlage nach Art. 44 ff. DSGVO.

(4) Als mögliche Transfergrundlagen kommen insbesondere ein einschlägiger Angemessenheitsbeschluss oder Standardvertragsklauseln mit erforderlichen ergänzenden Maßnahmen in Betracht. Eine bestimmte Transfergrundlage wird nicht pauschal zugesichert; maßgeblich ist die im konkreten Dienst tatsächlich anwendbare und eingesetzte Grundlage.

(5) Der Auftragsverarbeiter prüft vor der Nutzung eines Dienstes mit Drittlandbezug die Voraussetzungen nach Art. 44 ff. DSGVO und dokumentiert die maßgebliche Transfergrundlage, soweit dies erforderlich ist. Der Verantwortliche wird über wesentliche Änderungen eines Drittlandbezugs oder der Transfergrundlage informiert und erhält eine angemessene Einspruchsmöglichkeit nach § 9.

(6) Eine Übermittlung an ein Drittland aufgrund einer gesetzlichen Verpflichtung bleibt unberührt. Soweit gesetzlich zulässig, informiert der Auftragsverarbeiter den Verantwortlichen vorab.

§ 16 Vergütung und Aufwendungsersatz

(1) Für die gewöhnliche Erfüllung dieser AVV, einschließlich der üblichen Verarbeitung im Supportfall, wird kein gesonderter Aufwendungsersatz geschuldet, sofern der Hauptvertrag nichts Abweichendes bestimmt.

(2) Angemessene und nachgewiesene Aufwände für Sonderleistungen, die über die gewöhnliche Vertragserfüllung hinausgehen, werden nur erstattet, wenn dies vor ihrer Erbringung ausdrücklich vereinbart wurde und gesetzlich zulässig ist.

(3) Sonderleistungen können insbesondere außergewöhnliche Sonderkontrollen, umfangreiche Datenaufbereitungen oder nicht vom Hauptvertrag erfasste Unterstützungsleistungen sein.

(4) Gesetzliche Unterstützungs- und Mitwirkungspflichten des Auftragsverarbeiters werden durch diese Kostenregelung nicht eingeschränkt.

§ 17 Haftung

(1) Die Parteien haften für die Einhaltung der ihnen nach DSGVO, sonstigem Datenschutzrecht, Hauptvertrag und dieser AVV obliegenden Pflichten nach den gesetzlichen Vorschriften.

(2) Eine eigenständige Haftungsbeschränkung zulasten zwingender Ansprüche aus der DSGVO oder sonstiger zwingender gesetzlicher Haftung wird durch diese AVV nicht vereinbart.

(3) Soweit der Hauptvertrag Haftungsregelungen enthält, gelten diese für diese AVV nur, soweit sie mit zwingendem Datenschutzrecht vereinbar sind. Zwingende Haftung, insbesondere nach Art. 82 DSGVO, bleibt unberührt.

(4) Die Parteien informieren einander unverzüglich über Umstände, die zu einer Haftung, Inanspruchnahme oder behördlichen Maßnahme im Zusammenhang mit der Auftragsverarbeitung führen können, soweit dies rechtlich zulässig ist.

§ 18 Laufzeit und Beendigung

(1) Diese AVV tritt mit Abschluss des Lizenzvertrags durch Bestellung oder Annahme des individuellen Angebots in Kraft und läuft während der Laufzeit des Hauptvertrags.

(2) Eine ordentliche Beendigung dieser AVV ist grundsätzlich nur gemeinsam mit dem Hauptvertrag möglich. Das Recht zur außerordentlichen Beendigung aus wichtigem Grund bleibt unberührt.

(3) Der Verantwortliche kann die Verarbeitung mit sofortiger Wirkung untersagen, wenn der Auftragsverarbeiter wesentliche Pflichten dieser AVV verletzt und die Verletzung nicht unverzüglich beseitigt wird oder eine weitere Verarbeitung unzumutbar ist.

(4) Nach Beendigung des Hauptvertrags verarbeitet der Auftragsverarbeiter personenbezogene Daten nur noch zur Rückgabe, Löschung, Nachweisführung oder aufgrund einer gesetzlichen Verpflichtung.

(5) Der Verantwortliche erteilt die Weisung zur Rückgabe oder Löschung innerhalb einer angemessenen Frist. Der Auftragsverarbeiter weist die Durchführung nach Maßgabe des § 13 nach.

(6) Gesetzlich zulässige Aufbewahrungspflichten bleiben unberührt. Nach ihrem Ablauf sind die Daten zu löschen oder zu anonymisieren.

§ 19 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser AVV bedürfen der Textform, soweit nicht eine strengere Form gesetzlich vorgeschrieben ist. Dies gilt auch für die Änderung dieses Textformerfordernisses.

(2) Bei Widersprüchen zwischen dieser AVV und dem Hauptvertrag geht diese AVV für datenschutzrechtliche Fragen der Auftragsverarbeitung vor. Im Übrigen bleibt der Hauptvertrag unberührt.

(3) Die Anlagen 1 bis 3 sind Bestandteil dieser AVV. Änderungen der Anlagen sind zulässig, soweit sie den Gegenstand und das Schutzniveau der Verarbeitung nicht unzulässig erweitern oder vermindern und die Informations- und Einspruchsrechte nach § 9 gewahrt werden.

(4) Sollte eine Bestimmung dieser AVV ganz oder teilweise unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung tritt die gesetzliche Regelung.

(5) Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss kollisionsrechtlicher Vorschriften, soweit zwingendes Datenschutzrecht nicht entgegensteht.

(6) Gerichtsstand und Erfüllungsort richten sich nach dem Hauptvertrag, soweit gesetzlich zulässig.

(7) Die Parteien bestätigen den Abschluss dieser AVV durch die gemeinsame elektronische Akzeptanz im Online-Shop oder durch die Annahme des individuellen Angebots, dem diese AVV als Anlage beigefügt ist.

Anlage 1 – Verarbeitungsbeschreibung

Diese Anlage konkretisiert den Gegenstand der Verarbeitung nach Art. 28 Abs. 3 DSGVO. Sie ist auf die Support-Auftragsverarbeitung für SMART-Pedigree beschränkt.

1. Parteien und Hauptvertrag

Verantwortlicher ist der jeweilige Lizenznehmer, der den Lizenzvertrag abschließt. Auftragsverarbeiter ist die PiehBerz IT-Solutions UG (haftungsbeschränkt), Bahnhofstraße 53, 64409 Messel.

Hauptvertrag ist der Lizenzvertrag, der durch die jeweilige Bestellung im Online-Shop oder durch die Annahme eines individuellen Angebots zustande kommt. Diese AVV wird mit dem Abschluss dieses Hauptvertrags geschlossen.

2. Gegenstand und Dauer

Gegenstand ist die Verarbeitung personenbezogener Daten bei IT-Support, Fehleranalyse, Fehlerbehebung und Bug-Reporting über Zammad, einschließlich technischer Kommunikation, der Dokumentation des Supportfalls und einer freiwillig übermittelten Sicherheitsprotokolldatei.

Die Verarbeitung beginnt mit dem Abschluss der AVV und endet grundsätzlich mit dem Hauptvertrag. Nachlaufende Verarbeitung ist nur für Rückgabe, Löschung, Nachweisführung oder gesetzlich zulässige Aufbewahrung erlaubt.

Die lokale Verarbeitung von Patientendaten in SMART-Pedigree und die Verarbeitung der Eingaben im Webfragebogen sind nicht Gegenstand dieser AVV. Der Webfragebogen verarbeitet Eingaben clientseitig im Browser; eine Übertragung an PiehBerz erfolgt nicht.

3. Zwecke und Verarbeitungshandlungen

Zwecke sind die Bearbeitung von Supporttickets, Fehleranalyse, Fehlerbehebung, Bug-Reporting, technische Kommunikation und Dokumentation des jeweiligen Supportfalls.

Verarbeitungshandlungen sind Erheben, Empfangen, Speichern, Ordnen, Auslesen, Abgleichen, Übermitteln innerhalb des Supportprozesses, Einschränken und Löschen.

Nicht zulässig sind eigene Zwecke des Auftragsverarbeiters, insbesondere Werbung, Profilbildung, Training von KI-Modellen oder sonstige Auswertung außerhalb des Supportprozesses.

4. Kategorien personenbezogener Daten

Namen; geschäftliche Kontaktdaten; Ticketinhalte; Kommunikationsdaten; technische Angaben; Fehlermeldungen; Screenshots; Logdateien; gegebenenfalls das lokale Sicherheitsprotokoll.

Das Sicherheitsprotokoll enthält keine Patientendaten, Dateinamen, Lizenzschlüssel oder Hardwarekennungen. Jeder Eintrag enthält Datum und Uhrzeit. Das Protokoll liegt im Datenordner von SMART-Pedigree auf den Systemen der Einrichtung, je nach Installation im Programmordner, in einem von der IT festgelegten Ordner oder im Benutzerprofil. Die Übermittlung erfolgt nur freiwillig im Rahmen eines Supportfalls.

Gesundheitsdaten und genetische Daten dürfen grundsätzlich nicht übermittelt werden. Werden sie vom Verantwortlichen dennoch proaktiv in einem Ticket oder Anhang übermittelt und besteht eine wirksame AVV, können sie im Rahmen des konkreten Supportfalls verarbeitet werden.

5. Kategorien betroffener Personen

Betroffen sind Beschäftigte und Ansprechpartner des Verantwortlichen sowie mittelbar Patienten, soweit sie entgegen der vorgesehenen Datenminimierung in Ticketinhalten oder Anhängen genannt werden.

6. Datenminimierung und Ausschlüsse

Der Verantwortliche übermittelt nur die für den Supportfall erforderlichen Daten. Patienten-, Gesundheits- und genetische Daten sowie nicht erforderliche Namen, Dateinamen, Inhalte und Anhänge sind vor Übermittlung möglichst zu entfernen, zu anonymisieren oder zu schwärzen.

Einrichtungen ohne aktive Lizenz, insbesondere Einrichtungen in der Testphase, verwenden ausschließlich den isolierten Support ohne AVV. Dieser Supportprozess ist technisch und organisatorisch von dem Supportprozess für Einrichtungen mit bestehender AVV getrennt. Über den isolierten Supportweg dürfen keine Patienten-, Gesundheits- oder genetischen Daten übermittelt werden.

7. Speicher- und Löschfristen

Supporttickets samt Inhalten und Anhängen: spätestens drei Jahre nach Ende des Kalenderjahres des finalen Abschlusses.

Sicherheitsmeldungen: drei Jahre zum Jahresende nach Abschluss der Bearbeitung; länger nur, soweit gesetzliche Dokumentationspflichten oder die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dies erfordern.

Anfragen ohne bestehende AVV: technisch und organisatorisch isoliert; spätestens sechs Monate nach Eingang gelöscht, sofern es sich nicht um eine Sicherheitsmeldung handelt.

Backups: tägliche Sicherung mit 7 Tages-Backups, 4 Wochen-Backups und 6 Monats-Backups; maximale Vorhaltezeit sechs Monate. Nach Ablauf werden sie gelöscht oder überschrieben, soweit keine gesetzliche oder dokumentierte sicherheits- oder wiederherstellungsbezogene Ausnahme besteht.

8. Besondere Supportfälle

Sicherheitsmeldungen werden in einer eigenen Gruppe des Ticketsystems verarbeitet und organisatorisch getrennt von den übrigen Supporttickets behandelt.

Anfragen ohne bestehende AVV werden in einem isolierten Supportprozess mit restriktiven Zugriffsrechten verarbeitet. Ein automatisierter Hinweis untersagt die Übermittlung von Patienten-, Gesundheits- und genetischen Daten.

Anlage 2 – Technische und organisatorische Maßnahmen

Die folgenden Maßnahmen gelten für die Support-Auftragsverarbeitung nach dieser AVV. Sie werden risikoorientiert fortentwickelt, ohne das vereinbarte Schutzniveau zu unterschreiten.

1. Standort, Hosting und Datenverarbeitung

(1) Das Ticketsystem wird auf einem VPS in einem deutschen STRATO-Rechenzentrum betrieben.

(2) Die Administration und der Support erfolgen ausschließlich aus Deutschland. Ein Zugriff aus Drittstaaten ist nicht vorgesehen.

(3) Die Supportsysteme sind logisch von sonstigen Systemen getrennt. Eine logische Mandantentrennung stellt sicher, dass Kunden mit bestehender AVV unter ihrer eigenen Organisation geführt werden und nur deren Tickets sehen.

(4) Cloudflare wird nicht für das Ticketsystem eingesetzt. Cloudflare wird ausschließlich für Turnstile auf der Website und auf Anmeldeformularen verwendet.

2. Zutritts- und Zugangskontrolle

(1) Der physische Zutritt zu den Hostingbereichen wird durch den Hostinganbieter nach dessen Sicherheits- und Zutrittskonzept kontrolliert.

(2) Die Administration ist auf autorisierte Personen beschränkt. Als autorisierte Personen für Administration und Support sind Daniel Pieh und Florian Berz vorgesehen.

(3) Die Anmeldung ist nur mit Zwei-Faktor-Authentifizierung möglich.

(4) Ein Zugriff auf Supportdaten erfolgt nur, wenn ein aktiver Supportfall besteht und der Zugriff für dessen Bearbeitung erforderlich ist.

(5) Berechtigungen werden nach dem Need-to-know-Prinzip vergeben und bei Wegfall des Bedarfs entzogen.

3. Zugriffskontrolle und Nachvollziehbarkeit

(1) Änderungen an Tickets werden im Ticketverlauf protokolliert; die Anmeldung ist nur mit Zwei-Faktor-Authentifizierung möglich.

(2) Für die Administration wird SSH ausschließlich schlüsselbasiert verwendet; Passwort-Login ist deaktiviert.

(3) Die Netzwerkzugriffe werden durch eine UFW-Firewall auf die erforderlichen Verbindungen beschränkt.

(4) Zammad und sonstige Supportsysteme werden durch restriktive Rollen- und Berechtigungskonzepte abgesichert.

4. Übertragungssicherheit

(1) Die Übertragung zwischen berechtigten Clients und dem Supportsystem wird durch TLS 1.2 oder TLS 1.3 geschützt.

(2) Administrative Verbindungen werden über abgesicherte SSH-Verbindungen mit autorisierten Schlüsseln hergestellt.

(3) Unverschlüsselte Übertragungen von Supportdaten werden vermieden. Personenbezogene Daten sollen ausschließlich über den vorgesehenen Supportweg übermittelt werden.

5. Speichersicherheit und Verschlüsselung

(1) Backups werden mit AES-256 verschlüsselt im deutschen STRATO-HiDrive-Objektspeicher abgelegt.

(2) Die Verschlüsselung schützt Backups gegen unberechtigte Einsichtnahme bei Speicherung und Übertragung, soweit die eingesetzten Komponenten dies technisch unterstützen.

(3) Zugriffe auf Ticketdaten und Backups sind auf berechtigte Administrations- und Supportzwecke beschränkt.

6. Verfügbarkeit, Wiederherstellbarkeit und Backups

(1) Es werden tägliche automatisierte Backups erstellt.

(2) Die Aufbewahrung umfasst nach dem vorgesehenen Sicherungsschema 7 Tages-Backups, 4 Wochen-Backups und 6 Monats-Backups.

(3) Die maximale Backup-Vorhaltezeit beträgt sechs Monate.

(4) Das Backup-Monitoring überwacht die Durchführung der Sicherungen. Bei Fehlern erfolgt eine E-Mail-Alarmierung an die hierfür vorgesehenen administrativen Stellen.

(5) Die Wiederherstellung wird bei Bedarf geprüft und dient der Aufrechterhaltung und Wiederherstellbarkeit des Supportsystems.

7. Änderungs-, Schwachstellen- und Patchmanagement

(1) Für Debian und die Zammad-Docker-Umgebung werden regelmäßig Sicherheitsupdates eingespielt, soweit sie für die eingesetzten Komponenten verfügbar und technisch vertretbar sind.

(2) Sicherheitsrelevante Hinweise werden bewertet und nach Risiko priorisiert bearbeitet.

(3) Änderungen an produktiven Systemen werden kontrolliert durchgeführt und, soweit angemessen, nachvollziehbar dokumentiert.

8. Privacy by Design und Datenminimierung

(1) Die Supportprozesse sind nach dem Prinzip der datenschutzfreundlichen Gestaltung organisiert.

(2) Der Verantwortliche wird technisch und organisatorisch darauf hingewiesen, keine Patienten-, Gesundheits- oder genetischen Daten in Supporttickets zu übermitteln.

(3) Nicht erforderliche Daten sollen vor Übermittlung entfernt, anonymisiert oder geschwärzt werden.

(4) Anfragen ohne bestehende AVV werden isoliert, restriktiv berechtigt und technisch sowie organisatorisch von AVV-Supportfällen getrennt verarbeitet.

9. Löschung und Aufbewahrung

(1) Supporttickets samt Inhalten und Anhängen werden spätestens drei Jahre nach Ende des Kalenderjahres des finalen Abschlusses gelöscht.

(2) Sicherheitsmeldungen werden drei Jahre zum Jahresende nach Abschluss der Bearbeitung gespeichert, länger nur, soweit gesetzliche Dokumentationspflichten oder die Rechtsverteidigung dies erfordern.

(3) Isolierte Anfragen ohne bestehende AVV werden spätestens sechs Monate nach Eingang gelöscht, sofern sie nicht als Sicherheitsmeldung verarbeitet werden.

(4) Backups werden spätestens sechs Monate nach ihrer Erstellung gelöscht oder überschrieben, soweit keine dokumentierte Ausnahme besteht.

10. Organisatorische Sicherheit

(1) Für Administration und Support bestehen Rollen- und Berechtigungskonzepte.

(2) Personen mit Zugriff auf personenbezogene Daten werden zur Vertraulichkeit verpflichtet.

(3) Datenschutz- und Sicherheitsvorfälle werden dokumentiert und nach einem geregelten Verfahren bearbeitet.

(4) Die Maßnahmen werden regelmäßig auf ihre Wirksamkeit überprüft und bei Bedarf angepasst.

Anlage 3 – Genehmigte Unterauftragsverarbeiter

Der Verantwortliche genehmigt die nachstehenden Unterauftragsverarbeiter ausschließlich für die jeweils beschriebenen Leistungen. Weitere Unterauftragsverarbeiter richten sich nach § 9. Soweit ein Dienst keinen Zugriff auf Supportdaten erhält, wird dies in der Tabelle ausdrücklich klargestellt.

Unterauftragsverarbeiter	Leistung und Standort	Datenschutz / Bemerkungen
STRATO GmbH, Otto-Ostrowski-Straße 7, 10249 Berlin	Cloud-Hosting des VPS, Betrieb des Ticketsystems, Backup-Speicher HiDrive und SMTP; Verarbeitung und Administration in Deutschland	Auftragsverarbeitungsvertrag vorhanden; deutsches Rechenzentrum; Backups mit AES-256 verschlüsselt
Cloudflare, Inc., 101 Townsend St, San Francisco, CA 94107, USA	Ausschließlich Turnstile auf der Website und auf Anmeldeformularen; nicht für das Ticketsystem	Kein Zugriff auf Supporttickets; möglicher Drittlandbezug; Nutzung nur im erforderlichen Umfang und mit einer im konkreten Dienst anwendbaren Grundlage nach Art. 44 ff. DSGVO
Zammad GmbH, Marienstraße 18, 10117 Berlin	Ausschließlich Abruf von Übersetzungsdaten der Zammad-Software über translations.zammad.org	Nach dem vorgesehenen technischen Ablauf werden hierbei keine personenbezogenen Daten übermittelt; Zammad GmbH ist für diesen Abruf kein Auftragsverarbeiter

1. Genehmigungsumfang

(1) Die Genehmigung umfasst nur die in der Tabelle beschriebenen Leistungen, Datenzugriffe und Standorte.

(2) Eine Änderung der Leistung, des Standorts oder des Drittlandbezugs ist nach § 9 anzuzeigen und kann einen Widerspruch des Verantwortlichen auslösen.

(3) Der Auftragsverarbeiter verpflichtet STRATO als Unterauftragsverarbeiter durch eine Vereinbarung nach Art. 28 DSGVO zu einem angemessenen Datenschutz- und Sicherheitsniveau.

(4) Cloudflare wird ausschließlich für Turnstile auf der Website und auf Anmeldeformularen eingesetzt und nicht für das Ticketsystem. Eine Übermittlung von Supporttickets oder deren Inhalten an Cloudflare findet nicht statt.

(5) Der Abruf von Übersetzungsdaten durch Zammad GmbH ist nach dem vorgesehenen technischen Ablauf datenfrei im Hinblick auf personenbezogene Daten. Sollte sich dies ändern, darf der Abruf erst nach datenschutzrechtlicher Prüfung und erforderlicher vertraglicher Absicherung fortgesetzt werden.

2. Änderungen und Einspruch

(1) Der Auftragsverarbeiter informiert den Verantwortlichen vorab in Textform über die beabsichtigte Hinzunahme oder Ersetzung eines Unterauftragsverarbeiters.

(2) Der Verantwortliche kann innerhalb einer angemessenen Frist aus datenschutzrechtlichen oder sicherheitsbezogenen Gründen Einspruch erheben. Die Parteien suchen bei einem berechtigten Einspruch eine zumutbare Lösung.