Auftragsbearbeitungsvereinbarung

Version 2.5

zwischen
MedFlex Schweiz AG, Schindellegi, Schweiz
als Auftragsbearbeiter

und

dem jeweiligen Kunden gemäss Hauptvertrag
als Verantwortlichem

(gemeinsam die Parteien)

Diese Auftragsbearbeitungsvereinbarung (ABV) ist Bestandteil des zwischen der MedFlex Schweiz AG, Schindellegi, Schweiz und dem jeweiligen Kunden geschlossenen Hauptvertrags. Als Hauptvertrag gilt insbesondere das vom Kunden angenommene bzw. unterzeichnete Angebot, das diese ABV in ihrer jeweils gültigen Fassung einbezieht.

Folgende Anlagen bilden Bestandteile dieser Auftragsbearbeitungsvereinbarung (**ABV**):

Anlage 1: Beschreibung der Datenbearbeitung
Anlage 2: Unterauftragsbearbeiter
Anlage 3: Technische und organisatorische Massnahmen

1. Definitionen

(a) Die folgenden Begriffe haben nachstehende Bedeutungen:

(i) Anwendbare Datenschutzgesetze: (1) die Verordnung (EU) 2016/679 (Datenschutzgrundverordnung; DSGVO), soweit sie auf die betreffende Bearbeitung Anwendung findet, (2) das Schweizer Bundesgesetz über den Datenschutz (DSG; SR 235.1) und die zugehörige Datenschutzverordnung (DSV; SR 235.11), (3) die jeweils anwendbaren kantonalen Datenschutzgesetze und -bestimmungen sowie (4) sonstige anwendbare Datenschutzgesetze; jeweils in der jeweils gültigen Fassung und soweit sie auf die Bearbeitung von Daten des Verantwortlichen durch den Verantwortlichen und/oder den Auftragsbearbeiter Anwendung finden;

(ii) Daten des Verantwortlichen: Personenbezogene Daten, die im Auftrag des Verantwortlichen (oder eines mit ihm verbundenen Unternehmens) durch oder für den Auftragsbearbeiter im Zusammenhang mit dem Hauptvertrag bearbeitet werden;

(iii) Eingeschränkte Übermittlung: eine Bekanntgabe von Daten des Verantwortlichen in ein Land, bei der nach den anwendbaren Datenschutzgesetzen zusätzliche Voraussetzungen oder Garantien für die grenzüberschreitende Datenbekanntgabe erforderlich sind;

(iv) Unterauftragsbearbeiter: jede Person (mit Ausnahme eines Mitarbeitenden des Auftragsbearbeiters oder eines seiner Unterbeauftragten), die vom Auftragsbearbeiter oder in dessen Auftrag mit der Bearbeitung von Daten des Verantwortlichen im Zusammenhang mit dem Hauptvertrag beauftragt wurde. Nicht als Unterauftragsbearbeiter gelten Anbieter von Nebenleistungen, sofern nicht systematisch auf Daten des Verantwortlichen zugegriffen wird (z.B. Wartungs- und Supportanbieter, Telekommunikations- und Postanbieter). Vorbehalten bleibt in diesen Fällen aber die Pflicht des Auftragsbearbeiters zur Gewährleistung angemessener Sicherheitsmassnahmen gemäss Ziff. 4 dieser ABV, welche durch den Auftragsbearbeiter auf Unterauftragsbearbeiter zu überbinden ist.

(b) Die Begriffe Verantwortlicher, Auftragsbearbeiter (bzw. Auftragsverarbeiter), betroffene Person, Mitgliedstaat, personenbezogene Daten, Verletzung des Schutzes personenbezogener Daten, Bearbeitung (bzw. Verarbeitung) und Aufsichtsbehörde haben die diesen Begriffen in den anwendbaren Datenschutzgesetzen zugewiesenen Bedeutungen.

(c) Soweit in dieser ABV nicht abweichend definiert, finden auf diese ABV im Übrigen die Definitionen des Hauptvertrages Anwendung.

2. Bearbeitung von Daten des Verantwortlichen

(a) Der Verantwortliche ist mit Bezug auf die Daten des Verantwortlichen ein Verantwortlicher und der Auftragsbearbeiter ein Auftragsbearbeiter im Sinne der anwendbaren Datenschutzgesetze. Der Auftragsbearbeiter bearbeitet personenbezogene Daten ausschliesslich im Auftrag und im Interesse des Verantwortlichen.

(b) Der Verantwortliche ist berechtigt, dem Auftragsbearbeiter verbindliche Weisungen betreffend die Bearbeitung der Daten des Verantwortlichen zu erteilen. Solche Weisungen sind in Textform (einschliesslich E-Mail) oder ggf. durch Änderung der entsprechenden Einstellungen in der Applikation des Auftragsbearbeiters zu erteilen und entsprechend zu dokumentieren. Weisungen können jederzeit in der gleichen Form geändert oder ersetzt werden. Soweit Weisungen in Systemen des Auftragsbearbeiters aufgezeichnet werden, sind diese Aufzeichnungen dem Verantwortlichen auf Anfrage zur Verfügung zu stellen.

(c) Der Auftragsbearbeiter verpflichtet sich:

(i) bei der Bearbeitung von Daten des Verantwortlichen die anwendbaren Datenschutzgesetze einzuhalten, einschliesslich aller anwendbaren Dokumentationspflichten; und

(ii) die Daten des Verantwortlichen nur gemäss dem Hauptvertrag, dieser ABV und den Weisungen und Instruktionen des Verantwortlichen zu bearbeiten, es sei denn, er sei durch anwendbares Recht zu einer anderen Bearbeitung verpflichtet; in diesem Fall hat der Auftragsbearbeiter den Verantwortlichen, soweit zulässig, möglichst frühzeitig vor Beginn der entsprechenden Bearbeitung zu informieren. In diesem Fall hat der Verantwortliche das Recht, den Hauptvertrag und diese ABV durch Mitteilung in Textform unter Einhaltung einer Frist von einem Monat zu kündigen. Diese Frist kann sich ggf. um die Dauer von Rückführungs- bzw. Migrationsarbeiten gemäss dem Hauptvertrag verlängern, sofern der Verantwortliche darauf nicht verzichtet, und ebenso nach Ziff. 13(a). Müsste der Auftragsbearbeiter vor Ablauf dieser Frist mit einer vertrags- oder weisungswidrigen Bearbeitung beginnen, verständigen sich die Parteien über das für den Schutz der betroffenen Daten des Verantwortlichen geeignete Vorgehen.

(d) Der Verantwortliche weist den Auftragsbearbeiter hiermit an (und ermächtigt den Auftragsbearbeiter,

jeden Unterauftragsbearbeiter anzuweisen), die Daten des Verantwortlichen zu bearbeiten und sie vorbehaltlich Ziff. 10 in andere Länder zu übermitteln, jeweils sofern und soweit dies für die Zwecke des Hauptvertrages erforderlich ist.

3. Vertraulichkeit; Personal des Auftragsbearbeiters

(a) Der Auftragsbearbeiter verpflichtet sich, alle Daten des Verantwortlichen streng vertraulich zu behandeln, wobei er jene Sorgfalt walten lässt, die erforderlich ist, um einen unbefugten Zugriff, eine unbefugte Nutzung oder eine unbefugte Offenlegung möglichst zu vermeiden. Etwaige strengere Vertraulichkeitspflichten nach dem Hauptvertrag bleiben vorbehalten.

(b) Der Auftragsbearbeiter verpflichtet sich, die Zuverlässigkeit aller Personen mit Zugang zu den Daten des Verantwortlichen zu gewährleisten und den Zugang auf Personen zu beschränken, die die betreffenden Daten des Verantwortlichen für die Zwecke des Hauptvertrages bearbeiten müssen. Alle diese Personen müssen angemessenen gesetzlichen oder vertraglichen Vertraulichkeitsverpflichtungen unterliegen.

4. Sicherheitsmassnahmen

(a) Der Auftragsbearbeiter verpflichtet sich, in Bezug auf die Daten des Verantwortlichen durch technische und organisatorische Massnahmen ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten, insbesondere (i) die gegebenenfalls im Hauptvertrag genannten Massnahmen und (ii) die in Anlage 3 aufgeführten Massnahmen zu treffen. Der Auftragsbearbeiter verpflichtet sich, einen geeigneten Prozess zu unterhalten, um die Wirksamkeit der technischen und organisatorischen Massnahmen regelmässig zu überprüfen und ggf. zu verstärken, um die angemessene Sicherheit der Daten des Verantwortlichen dauerhaft zu gewährleisten. Anpassungen teilt der Auftragsbearbeiter dem Verantwortlichen in Textform mit.

(b) Der Auftragsbearbeiter unterstützt den Verantwortlichen angemessen, damit dieser seinen eigenen Verpflichtungen zur Aufrechterhaltung geeigneter technischer und organisatorischer Sicherheitsmassnahmen nachkommen kann.

5. Beizug von Unterauftragsbearbeitern

(a) Der Verantwortliche ermächtigt hiermit den Auftragsbearbeiter, nachstehende Personen mit der Bearbeitung von Daten des Verantwortlichen zu beauftragen:

(i) jeden der in Anlage 2 genannten Unterauftragsbearbeiter für die dort aufgeführten Leistungen und

(ii) jeden weiteren Unterauftragsbearbeiter, sofern dieser in Übereinstimmung mit dieser Ziff. 5 (und gegebenenfalls weiteren im Hauptvertrag enthaltenen Bedingungen) beauftragt wird.

(b) Mindestens zwei Wochen vor dem vorgesehenen Einsatz eines neuen Unterauftragsbearbeiters (oder eines bestehenden Unterauftragsbearbeiters für weitergehende Bearbeitungen) hat der Auftragsbearbeiter dem Verantwortlichen die Identität des betreffenden Unterauftragsbearbeiters und die Einzelheiten der von diesem durchzuführenden Bearbeitung in Textform mitzuteilen.

(c) Falls der Verantwortliche innerhalb von zwei Wochen nach Erhalt der vorgenannten Mitteilung der vorgeschlagenen Ernennung in Textform widerspricht, werden die Parteien in guten Treuen eine für beide Parteien akzeptable Alternative suchen. Können sich die Parteien innerhalb von zwei Monaten nach Mitteilung des Widerspruchs nicht auf eine Alternative einigen, hat der Verantwortliche das Recht, sämtliche Dienstleistungen, für welche Daten des Verantwortlichen von dem neuen Unterauftragsbearbeiter bearbeitet würden, ohne Kostenfolgen zu kündigen. Der Auftragsbearbeiter ist in diesem Fall verpflichtet, mit den betroffenen Daten des Verantwortlichen nach Ziff. 8 zu verfahren.

(d) Der Auftragsbearbeiter ist mit Bezug auf jeden Unterauftragsbearbeiter verpflichtet:

(i) mit dem Unterauftragsbearbeiter einen schriftlichen Vertrag zu schliessen, der den anwendbaren Datenschutzgesetzen genügt und ein Schutzniveau festlegt, das dem in dieser ABV und ggf. dem Hauptvertrag dargelegten Niveau mindestens gleichwertig ist;

(ii) sicherzustellen, dass der Unterauftragsbearbeiter das gemäss den anwendbaren Datenschutzgesetzen erforderliche und in dieser ABV und ggf. im Hauptvertrag geforderte Schutzniveau während der Dauer seiner Bearbeitung von Daten des Verantwortlichen gewährleistet. Auf Anfrage ist der Verantwortliche über die entsprechende Prüfung des Unterbeauftragten angemessen zu dokumentieren;

(iii) sicherzustellen, dass im Fall einer zulässigen eingeschränkten Übermittlung die nach Ziff. 10 erforderlichen Garantien vereinbart und eingehalten werden; und

(iv) dem Verantwortlichen auf dessen Verlangen Kopien der Vereinbarungen mit Unterauftragsbearbeitern zur Verfügung zu stellen (ggf. ohne

vertrauliche Informationen, die für die Anforderungen dieser ABV nicht relevant sind).

(e) Der Auftragsbearbeiter trifft die erforderlichen Massnahmen, um sicherzustellen, dass jeder Unterauftragsbearbeiter die Daten des Verantwortlichen nur in Übereinstimmung mit den etwaigen Vorgaben des Hauptvertrags, den Vorgaben dieser ABV und den Weisungen des Verantwortlichen bearbeitet. Verletzungen eines Unterauftragsbearbeiters werden dem Auftragsbearbeiter zugerechnet.

(f) Ein Prüfrecht gemäss Ziff. 9 gegenüber den Unterauftragsbearbeitern übt der Verantwortliche aus, indem er den Auftragsbearbeiter anweist, dessen Prüfrecht gegenüber dem Unterauftragsbearbeiter auszuüben. Der Verantwortliche kann vom Auftragsbearbeiter eine Kopie der Prüfungsergebnisse verlangen.

6. Betroffenenrechte; Kooperation

(a) Der Auftragsbearbeiter verpflichtet sich, den Verantwortlichen bei der Beantwortung von Anfragen betroffener Personen angemessen zu unterstützen. Der Auftragsbearbeiter ist insbesondere verpflichtet:

(i) den Verantwortlichen unverzüglich zu informieren, falls der Auftragsbearbeiter oder ein Unterauftragsbearbeiter eine Anfrage einer betroffenen Person erhält, die sich auf Daten des Verantwortlichen bezieht; und

(ii) Anfragen betroffener Personen ausschliesslich nach den Weisungen des Verantwortlichen oder den Anforderungen der anwendbaren Datenschutzgesetze (in welchem Fall der Auftragsbearbeiter diese Anforderungen dem Verantwortlichen vorab mitteilt) zu beantworten.

(b) Der Auftragsbearbeiter verpflichtet sich, den Verantwortlichen mit Bezug auf Daten des Verantwortlichen bei der Durchführung von Datenschutz-Folgeabschätzungen und bei Konsultationen mit Aufsichtsbehörden oder anderen zuständigen Behörden angemessen zu unterstützen.

(c) Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich, soweit dies nach dem anwendbaren Recht zulässig ist, (i) wenn sich eine Aufsichtsbehörde im Zusammenhang mit der Bearbeitung von Daten des Verantwortlichen direkt an den Auftragsbearbeiter wendet und/oder (ii) wenn die Daten des Verantwortlichen durch eine Beschlagnahme, ein Konkursverfahren oder ein ähnliches Ereignis betroffen sind oder zu sein drohen. In letzterem Fall hat der Auftragsbearbeiter jeden an solchen Massnahmen beteiligten Dritten (einschliesslich Behörden) darüber in Kenntnis zu setzen, dass die Kontrolle über die Daten des Verantwortlichen beim Verantwortlichen liegt.

(d) Der Auftragsbearbeiter legt Daten des Verantwortlichen nur mit vorgängiger schriftlicher Zustimmung durch den Verantwortlichen an Behörden (einschliesslich von Gerichten, Verwaltungs- und Strafverfolgungsbehörden) offen oder wenn er dazu rechtlich verpflichtet ist. Wird der Auftragsbearbeiter zu einer solchen Offenlegung aufgefordert, informiert er den Verantwortlichen unverzüglich, soweit ihm dies nicht verbindlich untersagt ist. Er ist verpflichtet, sämtliche zur Verfügung stehenden Rechtsmittel gegen eine solche Aufforderung einzulegen, soweit ihn der Verantwortliche nicht anders anweist, und den Verantwortlichen über den weiteren Verlauf zu unterrichten. Ziff. 2(c)(ii) bleibt vorbehalten.

7. Datenschutzverletzungen

(a) Der Auftragsbearbeiter verpflichtet sich, den Verantwortlichen unverzüglich, spätestens aber innert 48 Stunden zu benachrichtigen, wenn er Kenntnis von einer Verletzung des Schutzes personenbezogener Daten erlangt. Der Auftragsbearbeiter hat dem Verantwortlichen insbesondere ausreichende Informationen zur Verfügung zu stellen, damit der Verantwortliche allfällige Pflichten zur Meldung der Verletzung personenbezogener Daten an eine Aufsichtsbehörde und/oder an betroffene Personen nach den anwendbaren Datenschutzgesetzen erfüllen kann.

(b) Der Auftragsbearbeiter verpflichtet sich, (i) den Verantwortlichen bei der Untersuchung, Eingrenzung und Behebung einer Verletzung des Schutzes personenbezogener Daten mit Bezug auf Daten des Verantwortlichen angemessen zu unterstützen und (ii) ohne vorherige ausdrückliche Zustimmung des Verantwortlichen in Textform keinen Dritten über eine Verletzung des Schutzes personenbezogener Daten zu informieren, sofern und soweit dies nach anwendbarem Recht nicht erforderlich ist.

8. Löschung und Rückgabe von Daten des Verantwortlichen

(a) Der Auftragsbearbeiter verpflichtet sich unter Vorbehalt von Ziff. 8(b) und 8(c), sämtliche Kopien der Daten des Verantwortlichen zu löschen und die Löschung durch jeden Unterauftragsbearbeiter zu veranlassen, sobald die Vertragsleistungen beendet werden, in deren Zusammenhang Daten des Verantwortlichen bearbeitet werden (Abschlussdatum), spätestens aber vier Wochen nach dem Abschlussdatum.

(b) Unter Vorbehalt von Ziff. 8(c) kann der Verantwortliche den Auftragsbearbeiter innerhalb von zwei Wochen nach dem Abschlussdatum in Textform anweisen, dem Verantwortlichen eine Kopie aller von ihm oder einem Unterauftragsbearbeiter bearbeiteten

Daten des Verantwortlichen in einem vom Verantwortlichen vernünftigerweise verlangten Dateiformat zu übermitteln. Einer solchen Anweisung ist innerhalb von vier Wochen seit dem Abschlussdatum zu entsprechen.

(c) Der Auftragsbearbeiter und jeder Unterauftragsbearbeiter ist berechtigt, Daten des Verantwortlichen in dem vom anwendbaren Recht geforderten Umfang aufzubewahren, sofern der Auftragsbearbeiter die Vertraulichkeit dieser Daten gewährleistet und sicherstellt, dass sie nur im notwendigen Umfang bearbeitet werden.

(d) Der Auftragsbearbeiter verpflichtet sich, dem Verantwortlichen innerhalb von fünf Wochen seit dem Abschlussdatum in Textform zu bestätigen, dass er seinen Verpflichtungen gemäss dieser Ziff. 8 nachgekommen ist.

(e) Retentionsrechte an Daten und Datenträgern des Verantwortlichen sind generell ausgeschlossen.

9. Audits

(a) Der Auftragsbearbeiter stellt dem Verantwortlichen auf Verlangen alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung dieser ABV nachzuweisen, und erlaubt dem Verantwortlichen, zu diesem Zweck vor Ort Audits durchzuführen oder durch einen Prüfer durchführen zu lassen. Er wirkt bei der Prüfung angemessen mit. Audits sind nach vorheriger Ankündigung während der üblichen Geschäftszeiten und ohne unangemessene Beeinträchtigung des Geschäftsbetriebes des Auftragsbearbeiters durchzuführen. Der Verantwortliche behandelt die vom Auftragsbearbeiter im Rahmen eines solchen Audits zur Verfügung gestellten Informationen vertraulich, ist aber berechtigt, diese ABV und Vereinbarungen zwischen dem Auftragsbearbeiter und Unterauftragsbearbeitern und weitere Informationen offenzulegen, wenn dies zum Nachweis der Erfüllung seiner datenschutzrechtlichen Pflichten erforderlich ist.

(b) Die Rechte nach Ziff. 9(a) gelten nur, soweit der Hauptvertrag dem Verantwortlichen nicht anderweitig den Anforderungen der anwendbaren Datenschutzgesetze genügende Informations- und Kontrollrechte einräumt.

10. Auslandsübermittlungen

(a) Personendaten dürfen ins Ausland bekanntgegeben werden, wenn dies nach den anwendbaren Datenschutzgesetzen zulässig ist. Soweit das Schweizer Datenschutzrecht Anwendung findet, ist eine Bekanntgabe insbesondere zulässig, wenn der Bundesrat für den Empfängerstaat ein angemessenes Datenschutzniveau festgestellt hat. Fehlt ein angemessenes Datenschutzniveau, stellt der Auftragsbearbeiter vor der Bekanntgabe geeignete Garantien gemäss Art. 16 Abs. 2 DSG sicher oder stützt die Bekanntgabe auf eine gesetzlich vorgesehene Ausnahme.

(b) Soweit die DSGVO auf eine Auslandsübermittlung Anwendung findet, werden zusätzlich die Anforderungen der Art. 44 ff. DSGVO eingehalten.

(c) Werden Standarddatenschutzklauseln verwendet, kommen die vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) anerkannten Standardvertragsklauseln der Europäischen Kommission in dem für die jeweilige Übermittlung einschlägigen Modul zur Anwendung. Die nach Schweizer Datenschutzrecht erforderlichen Anpassungen und Ergänzungen werden berücksichtigt. Soweit ausschliesslich Schweizer Datenschutzrecht anwendbar ist, gilt der EDÖB als zuständige Aufsichtsbehörde; die Rechte betroffener Personen nach Schweizer Recht bleiben einschliesslich des Zugangs zu den zuständigen Schweizer Gerichten unberührt.

(d) Der Auftragsbearbeiter stellt sicher, dass auch Unterauftragsbearbeiter und allfällige Weiterübermittlungen die Anforderungen dieser Ziff. 10 einhalten.

(e) Der Auftragsbearbeiter führt keine eingeschränkte Übermittlung ohne geeignete Garantien im Sinne der anwendbaren Datenschutzgesetze durch. Er stellt dem Verantwortlichen auf Anfrage die für die Prüfung dieser Garantien erforderlichen Informationen zur Verfügung.

(f) Der Auftragsbearbeiter darf ohne vorgängige Zustimmung des Verantwortlichen in Textform keine eingeschränkten Übermittlungen ausführen, wobei diese Zustimmung nicht unangemessen verweigert werden darf. Vorbehalten bleibt Ziff. 5, sofern sämtliche Anforderungen dieser Ziff. 10 erfüllt sind.

11. Haftung; Schadloshaltung

(a) Unter Vorbehalt von Ziff. 11(b) und unter Vorbehalt vorsätzlicher oder grobfahrlässiger Verletzungen schliessen die Parteien gegenseitig jede Haftung für Verletzungen dieser ABV im gesetzlich zulässigen Rahmen aus.

(b) Der Auftragsbearbeiter verpflichtet sich gegenüber dem Verantwortlichen, den Verantwortlichen und die mit ihm verbundenen Unternehmen sowie deren jeweiligen Organe, Mitarbeitende, Vertreter und Auftragnehmer (jeweils eine freizustellende Partei) von sämtlichen Verlusten, Schäden und Kosten, einschliesslich angemessener Anwalts- und Verfahrenskosten, die sich aus Ansprüchen Dritter gegen eine freizustellende Partei im Zusammenhang mit der Nichteinhaltung von Verpflichtungen des Auftragsbe-

arbeiters bei der Bearbeitung von Daten des Verantwortlichen ergeben, vollumfänglich schadlos zu halten. Weitergehende Freistellungs- und Schadloshaltungspflichten nach dem Hauptvertrag bleiben vorbehalten.

12. Change of Control und Werbenutzung

Unternehmensübernahme: Im Falle einer Unternehmensübernahme, eines Verkaufs oder einer vergleichbaren Veränderung der Eigentumsverhältnisse des Auftragsbearbeiters (Change of Control) gilt:

(a) Der Auftragsbearbeiter informiert den Verantwortlichen über einen Change of Control, soweit rechtlich zulässig, möglichst frühzeitig und grundsätzlich mindestens 30 Tage vor dessen Wirksamwerden. Ist eine vorherige Information aus rechtlichen oder vertraglichen Gründen nicht zulässig, erfolgt die Information unverzüglich nach Wegfall des Hinderungsgrundes.

(b) Soweit der Change of Control mit einer Übertragung der Vertragsstellung oder von Daten des Verantwortlichen auf eine andere juristische Person verbunden ist, stellt der Auftragsbearbeiter sicher, dass der Erwerber in die bestehenden vertraglichen Datenschutzpflichten eintritt oder ein mindestens gleichwertiges Datenschutzniveau gewährleistet.

(c) Der Verantwortliche hat im Falle eines Change of Control ein ausserordentliches Kündigungsrecht mit einer Frist von 30 Tagen ab Kenntnisnahme.

(d) Im Falle einer Kündigung aufgrund eines Change of Control erfolgen Datenrückgabe und Löschung gemäss Ziff. 8 ohne zusätzliche Kosten.

Ausschluss der Werbenutzung: Der Auftragsbearbeiter ist nicht berechtigt, Personendaten des Verantwortlichen für eigene Werbezwecke, zur Profilbildung, für Marktforschung, zur Produktentwicklung oder für sonstige kommerzielle Zwecke ausserhalb des Hauptvertrags zu nutzen. Dies gilt auch im Falle eines Change of Control und für Rechtsnachfolger des Auftragsbearbeiters.

13. Dauer und Beendigung

(a) Diese ABV tritt mit ihrer Einbeziehung in den Hauptvertrag, spätestens aber mit dem erstmaligen Zugriff des Auftragsbearbeiters auf Daten des Verantwortlichen in Kraft und endet mit der Beendigung der Vertragsleistungen, in jedem Fall aber frühestens mit der Löschung der Daten des Verantwortlichen.

(b) Der Verantwortliche ist zur fristlosen Kündigung dieser ABV und des Hauptvertrags aus wichtigem Grund berechtigt, wenn der Auftragsbearbeiter schwerwiegend gegen die Bestimmungen dieser ABV verstösst, eine rechtmässige Weisung des Verantwortlichen nicht ausführen kann oder will oder die Prüfrechte des Verantwortlichen vertragswidrig verweigert.

14. Rangfolge

(a) Diese ABV schränkt die Pflichten des Auftragsbearbeiters nach dem Hauptvertrag mit Bezug auf den Schutz personenbezogener Daten nicht ein und erlaubt dem Auftragsbearbeiter nicht, personenbezogene Daten zu bearbeiten oder bearbeiten zu lassen, soweit dies gegen den Hauptvertrag verstossen würde.

(b) Im Fall eines Widerspruchs gehen die Standardvertragsklauseln (soweit vereinbart) dieser ABV vor (wobei diese ABV als ergänzende Regelung der Standardvertragsklauseln anwendbar bleibt) und geht diese ABV dem Hauptvertrag und allen anderen Vereinbarungen zwischen den Parteien (auch nach dieser ABV geschlossenen Vereinbarungen) vor.

15. Schlussbestimmungen

(a) Der Verantwortliche ist berechtigt, den Hauptvertrag und/oder diese ABV mit Mitteilung in Textform mindestens 30 Tage im Voraus anzupassen, soweit dies zur Einhaltung der anwendbaren Datenschutzgesetze oder einer verbindlichen Anordnung einer Behörde erforderlich ist.

(b) Die Erfüllung dieser ABV ist durch die im Hauptvertrag vereinbarte Vergütung (auch wenn keine Vergütung vereinbart wurde) vollständig abgegolten. Es besteht kein Anspruch auf Kostenersatz.

(c) Die Bestimmungen des Hauptvertrages betreffend anwendbares Recht und Gerichtsstand finden auf diese ABV Anwendung, unter dem Vorbehalt, dass der Verantwortliche berechtigt bleibt:

(i) eine vorsorgliche Massnahme vor jedem zuständigen Gericht zu beantragen; und

16. Klage gegen den Auftragsbearbeiter in einem Drittverfahren unter Beteiligung des Verantwortlichen zu erheben, sofern und soweit dies nach dem anwendbaren Verfahrensrecht zulässig ist.

Anlage 1: Beschreibung der Datenbearbeitung

Punkt	**Beschreibung**
Beschreibung der Bearbeitungen und Zwecke:	Die Bearbeitungen und die Bearbeitungszwecke ergeben sich aus dem Hauptvertrag.
Betroffene Personen:	Die von der Datenbearbeitung im Auftrag des Verantwortlichen betroffenen Personen ergeben sich aus dem Hauptvertrag.
Personenbezogene Daten:	Die Kategorien der im Auftrag des Verantwortlichen bearbeiteten personenbezogenen Daten ergeben sich aus dem Hauptvertrag.
Besondere Kategorien personenbezogener Daten (besonders schützenswerte Personendaten):	Die im Zusammenhang mit dem Hauptvertrag bearbeiteten besonders schützenswerten Personendaten ergeben sich aus dem Hauptvertrag.
Dauer der Speicherung der Daten oder zumindest die Kriterien für die Festlegung dieser Dauer	Die Dauer der Speicherung richtet sich nach dieser Auftragsbearbeitungsvereinbarung und dem Hauptvertrag.

Anlage 2: Unterauftragsbearbeiter

Der Auftragsbearbeiter ist berechtigt, die folgenden Unterauftragsbearbeiter nach Massgabe von Ziff. 5 der ADV mit Bezug auf die folgenden Leistungen neu bzw. weiterhin zu beauftragen:

Hosting

Name	Anschrift	Funktion	Ort der Verarbeitung
medflex GmbH	medflex GmbH, Reichenaustraße 39a, 78467 Konstanz, Deutschland	Technischer Betrieb und Bereitstellung der medflex Plattform	Deutschland
OVHcloud	OVH GmbH, St. Johanner Str. 41-43, 66111 Saarbrücken, Deutschland	Rechenzentrum	EU

Kommunikationsdienste

Name	Anschrift	Funktion	Ort der Verarbeitung
Arzt-konsultation[1]	arztkonsultation ak GmbH, Schusterstr. 3, 19055 Schwerin, Deutschland	Video Kommunikation API	EU

Telefonassistent

Name	Anschrift	Funktion	Ort der Verarbeitung
Microsoft[2]	Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park, Dublin D18 P521, Irland	Terminbuchung Transkription	EU
Twilio[2]	Twilio Germany GmbH, Unter den Linden 10, 10117 Berlin, Deutschland	Anrufverwaltung des Telefonassistenten	EU
ElevenLabs[3]	ElevenLabs Poland LLC, Lipska 27/22, 03-907 Warschau, Polen	Kommunikationsagent	EU

Zustimmungsverwaltung

Name	Anschrift	Funktion	Ort der Verarbeitung
CCM19	Papoo Software & Media GmbH, Auguststr. 4, 53229 Bonn, Deutschland	Zustimmungs-verwaltung	EU

Benachrichtungsdienste

Name	Anschrift	Funktion	Ort der Verarbeitung
Cleverpush	CleverPush GmbH, Brauhausstr. 15A, 22041 Hamburg, Deutschland	Benachrichtigungen	EU
Brevo	Sendinblue GmbH, Köpenicker Str. 126, 10179 Berlin, Deutschland	Benachrichtigungen	EU
smsmode	Calade Technologies SARL, 4 rue Duverger, 13002 Marseille, Frankreich	Benachrichtigungen	EU

[1] Betrifft nur den Video-Messenger

[2] Betrifft nur das Zusatzmodul Telefonassistent

[3] Betrifft nur den Telefonassistenten mit interaktiver Gesprächsführung

Anlage 3: Technische und organisatorische Massnahmen

Die medflex GmbH hat die innerbetriebliche Organisation so gestaltet, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

Die Überwachung der Einhaltung datenschutzrechtlich geforderter Maßnahmen erfolgt im Rahmen eines Datenschutz-Managementsystems durch den Datenschutzbeauftragten der medflex sowie der zuständigen Aufsichtsbehörde.

Rechenzentren

Informationen zum Standort von Datenverarbeitungsanlagen und Rechenzentren	Der Standort der Rechenzentren (RZ) liegt bei der OVHcloud. Die RZ befinden sich in der EU, genutzt werden deutsche RZ. Für die Backups werden französische RZ genutzt. Weitere Datenverarbeitungen finden in-House statt, ein eigenes Rechenzentrum wird nicht betrieben.

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle (Kein unbefugter Zutritt zu Datenverarbeitungsanlagen)	Zentraler Empfang für Besucher und Dienstleister Organisatorische Besucherregelung (Begleitung von Besuchern und Fremdpersonal) Einsatz elektronischer Schließsysteme mit Zugangs-Batches und Protokollierung der Zutritte Serverraum mit gesondertem Schließbereich Zutrittskontrollsystem: Ausweisleser, Magnetkarte, Chipkarte Schlüssel / Schlüsselvergabe Türsicherung (elektrische Türöffner usw.) Gebäudesicherung (Pforten) Überwachungseinrichtung: Alarmanlage Alarmsicherung Schließsystem
Zugangskontrolle (Keine unbefugte Systembenutzung)	Zentrale Serververwaltung in einem gesicherten Serverraum Organisatorische Anweisungen zum Einsatz von IT-Systemen Räumliche Trennung der Produktivsysteme und der Datensicherungsmedien, die unter Verschluss gehalten werden Organisationsanweisung für Telearbeitsplätze inkl. VPN-Zugang mit Zwei-Faktor-Identifizierung Organisationsanweisungen für die Ablage, Lagerung und Entsorgung von Speichermedien und ausgedruckten Unterlagen Einsatz mehrstufiger Authentifizierungsverfahren (Passwortabfragen) Login-Protokollierungen (Sperrung bei Überschreitung der Anzahl gesetzter Fehlversuche)

	Organisationsanweisung zur Passwortnutzung (Mindestlänge, Restriktionen) Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts) Einrichtung eines Benutzerstammsatzes pro User Verschlüsselung von Datenträgern Software Firewall Hardware Firewall Einsatz von zentraler Administrations-Software für mobile Endgeräte (z.B. zum externen Sperren und Löschen von Daten) Gehäuseschutz Schutzmaßnahmen zur Sicherung bei Nutzung von eigenen Geräten durch Mitarbeiter (z.B. Fernlöschung oder -sperrung) Anti-Viren Software
Zugriffskontrolle (Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems)	Persönliche Benutzerkonten, individuelle Berechtigungen Einsatz eines mehrstufigen Berechtigungssystems Bedarfsgerechte Beschränkungen der Benutzerrechte und Freigaben auf Verzeichnis- und Dateiebene (z. B. lesen, schreiben) Einsatz kryptographischer Verfahren mit Benutzerauthentifizierung (Festplattenverschlüsselung, Verschlüsselung einzelner Verzeichnisse, VPN) Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte (Profile, Rollen, Transaktionen und Objekte) Benutzerkennung mit Passwort Virenschutz / Firewall Regelmäßige Updates der Systeme Klassische Rollen (Auswertungen, Kenntnisnahme, Veränderung, Löschung) Protokollierung von Zugriffen in Logs
Trennungskontrolle / Verwendungszweckkontrolle (Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden)	Einrichtung projektbezogener Ordnerstrukturen Mandantentrennung durch zumindest logische Datentrennung Vorhandene Datenbestände werden ausschließlich im Rahmen der vertraglichen Zweckbestimmung und auf Weisung des Auftraggebers verwendet Trennung von Produktiv- und Testsystemen Zweckbindung Separierung Datenbanken Separierung von Tables in Datenbanken Funktionstrennung / Produktion / Test & Sandboxing

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle (Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport)	Datenweitergaben an Dritte erfolgen grundsätzlich nicht. Ausnahmen sind: Gesetzlich vorgeschriebene Datenweitergaben im Zuge von Ermittlungsverfahren strafverfolgender Behörden oder bei einer vertraglich vereinbarten Weitergabe an beauftragte Subunternehmen. Daten, die aufgrund von gesetzlichen Vorgaben an die entsprechenden Stellen zu übertragen sind, wie zum Beispiel Steuer- und Sozialversicherungsdaten, werden auf den durch den Gesetzgeber vorgeschriebenen Wegen und mit den dort vorgegebenen Verschlüsselungen übertragen. Einsatz von kryptographischen Verfahren (Datenverschlüsselung) auf der gesamten Datenverbindungsstrecke (Nutzung VPN, Einsatz kundenspezifischer Verschlüsselungs-/ Sicherheitstechniken ggf. mit separatem Austausch von Kennwörtern/Schlüsseln über sichere Kommunikationsverbindungen). Protokollierung https- und E-Mail Datenverkehr ein- und ausgehend. Transport von Datenträgern nur innerhalb gesicherter Räume bzw. bei Versand durch Kurier oder persönlicher Übergabe an berechtigte Personen. Elektronische Datenträger werden vor dem Versand verschlüsselt, die Entsorgung von Datenträgern erfolgt durch physikalische Zerstörung des Speichermediums. Papierunterlagen werden in geeigneten Entsorgungsbehältern gesammelt und durch fachkundiges Personal vernichtet. Regelungen zur Wartung und den Schutz der Vertraulichkeit im Rahmen von Reparaturen oder Außerbetriebnahmen sind organisatorisch geregelt. Verschlüsselung / Tunnelverbindung Prüfung der Rechtmäßigkeit der Weitergabe von Daten Regelungen zum datenschutzkonformen Vernichten von Datenträgern Verfahrensverzeichnis Protokollierung Transportsicherung
Eingabekontrolle (Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind)	Organisatorische Festlegung von Zuständigkeiten Zugriffssteuerung von Serverzugriffen Eine Eingabekontrolle auf Ebene der einzelnen Datenfelder ist mit vertretbarem Aufwand in der vorhandenen Individualanwendung zur Datenverarbeitung derzeit nicht möglich. Wo immer möglich und sinnvoll, werden daher organisatorische Verfahren umgesetzt, die geeignet sind, den Personenkreis, der eine Änderung oder Löschung personenbezogener Daten im Rahmen der Auftragsdatenverarbeitung durchführen kann, zu begrenzen. Sicherung von Protokolldaten gegen Verlust oder Veränderung

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b, c DSGVO)

Verfügbarkeitskontrolle (Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust)	Es erfolgt eine regelmäßige Datensicherung mit täglichen, wöchentlichen und monatlichen inkrementellen und vollständigen Sicherungen. Die Sicherungen werden zudem entsprechend den gesetzlichen Aufbewahrungsfristen archiviert. Organisationsanweisung zur strukturierten Datenhaltung auf zentralen Serversystemen Betrieb der zentralen Serversysteme innerhalb besonders geschützter Umgebung Räumlich getrennte Aufbewahrung von Produktivsystemen und Datensicherungsmedien Die IT-Systeme verfügen über technische Systeme (z. B. Redundanz) zur Erhöhung der Ausfallsicherheit und sind an einer unterbrechungsfreien Stromversorgung (USV) angeschlossen. Der Serverraum verfügt über angemessene Peripheriesysteme zur Brandfrüherkennung und zur Klimatechnik. Backup-Strategie (offline) Backup-Strategie (online, z.B. Cloud) Unterbrechungsfreie Stromversorgung (USV) Getrennte Aufbewahrung Überspannungsschutz Schutz vor Diebstahl Virenschutz / Firewall
Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO - die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen)	Anleitungen zur Interpretation von Notfall-Signalen und deren korrekter Behebung (z.B. Server-Neustart, Server-Skalierung bei Hochlast, Wiederherstellung von Backups). Notfallmanagement inkl. Notfallpläne Testen der Wiederherstellungssysteme

Technische und organisatorische Umsetzung des Rechts auf Löschung (Art. 17 DSGVO)

Folgende Maßnahmen wurden ergriffen	Einfache Datenlöschung (ohne Überschreiben) Randomisiertes Überschreiben von Datensätzen Implementierung von Fernlöschung, z.B. auf mobilen Endgeräten Zerstörung von Datenträgern vor der Entsorgung Schreddern / mechanische Deformierung von Datensätzen auf Papier / DVD / CD oder sonstigen Datenträgern Automatische Löschung von Datensätzen nach einem festgelegten Ablaufdatum Sorgfältige Auswahl von Entsorgungsdienstleistern Protokollierung von Löschvorgängen

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags Verpflichtung der Mitarbeiter auf Wahrung der Vertraulichkeit, das Datengeheimnis und den Datenschutz Die Regelungen werden regelmäßig auf Aktualität geprüft Für spezielle Bereiche, Personal, gibt es eigenständige Regelungen Die Wirksamkeit der Regelungen wird bei Bedarf durch Datenschutzaudits festgestellt Ein Handlungsrahmen für die Beschäftigten im Umgang mit personenbezogenen Daten ist als Datenschutzrichtlinie veröffentlicht Datenschutz-Managementsystem Ein Datenschutzbeauftragter ist bestellt Eine Auftragskontrolle der Dienstleister wird durch den Datenschutzbeauftragten durchgeführt, z.B. mit Überprüfungen der Dienstleister Regelmäßige Datenschutzschulungen Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO) Auftragskontrolle (AV) Eindeutige Vertragsgestaltung Datenschutzfreundliche Voreinstellungen (Privacy by Design / Privacy by Default) Nachkontrollen

Gesamtevaluierung der Maßnahmen

Die dokumentierten Maßnahmen sind unter Berücksichtigung des aktuellen Standes der Technik, angemessener Implementierungs- und Wartungskosten, der Art, des Umfangs und der Zwecke der Verarbeitung, sowie unter Abwägung der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.