Auftragsdatenverarbeitungsvertrag (AVV) medidux™

zwischen

[Name Kundin]
[Adresse]
[PLZ Ort]
Schweiz

nachfolgend „Auftraggeberin“

und

mobile Health AG
Mühlebachstrasse 43
8008 Zürich
Schweiz

nachfolgend „Auftragsbearbeiterin“

gemeinsam die „Parteien“

Inhalt

1. Zweck der Vereinbarung 3
2. Rollen der Parteien 3
3. Gegenstand, Art und Zweck der Datenbearbeitung 3
4. Kategorien von Personendaten 4
5. Kategorien betroffener Personen 5
6. Dauer der Bearbeitung 5
7. Weisungen der Auftraggeberin 5
8. Pflichten der Auftraggeberin 5
9. Pflichten der Auftragsbearbeiterin 6
10. Vertraulichkeit 6
11. Ort der Datenbearbeitung 6
12. Unterauftragnehmer 6
13. Technische und organisatorische Massnahmen 7
14. Meldung von Datenschutzverletzungen 7
15. Unterstützung bei der Geltendmachung von Betroffenenrechten 8
16. Unterstützung bei Datenschutzpflichten 8
17. Prüfrechte 8
18. Rückgabe und Löschung nach Ende der vertraglichen Beziehungen 8
19. Nutzung anonymisierter oder aggregierter Daten 9
20. Haftung 9
21. Schlussbestimmungen 9

1. Zweck der Vereinbarung

Diese Auftragsdatenbearbeitungsvereinbarung regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Bearbeitung von Personendaten durch die Auftragsbearbeiterin im Auftrag der Auftraggeberin im Zusammenhang mit der Nutzung von medidux™.

Sie ergänzt das Angebot, die Allgemeinen Vertragsbedingungen / Nutzungsbedingungen medidux™ SaaS sowie allfällige weitere Vereinbarungen zwischen den Parteien.

Soweit diese Vereinbarung im Verhältnis zu den vorstehend genannten Dokumenten abweichende Regelungen enthält, gehen diese vor.

2. Rollen der Parteien

Die Auftraggeberin entscheidet im Rahmen der Nutzung von medidux™ über Zweck und Mittel der Bearbeitung von Patienten- und anderen Personendaten und ist insoweit datenschutzrechtlich Verantwortliche.

Die Auftragsbearbeiterin bearbeitet Personendaten im Auftrag der Auftraggeberin und nach deren Weisung, soweit sie nicht ausnahmsweise eigene gesetzliche Pflichten oder eigene Verantwortlichkeiten wahrnimmt.

3. Gegenstand, Art und Zweck der Datenbearbeitung

Gegenstand der Datenbearbeitung ist die technische Bereitstellung, Speicherung, Übermittlung, Anzeige, Unterstützung, Sicherung und Auswertung von Daten im Rahmen der vereinbarten Nutzung von medidux™.

Die Bearbeitung erfolgt insbesondere zum Zweck:

- der Bereitstellung der medidux™ Plattform,
- der strukturierten Erfassung patientenbezogener Angaben,
- der Darstellung von Symptom-, Vital-, Medikations-, Verlaufs-, Fragebogen-, Labor- und Diagnostikdaten,
- der Verarbeitung, Darstellung, Übermittlung und Speicherung von Labor- und Diagnostikdaten, soweit dies im vereinbarten Leistungsumfang, über manuelle Eingaben, Uploads oder angebundene Schnittstellen vorgesehen ist,
- der Unterstützung von Kommunikation und Betreuung durch die Auftraggeberin,
- der Verarbeitung, Darstellung, Übermittlung und Speicherung von Genomik-, Molekularpathologie-, Biomarker-, Formular-, Register-, Studien- sowie Board- und Konsildaten, soweit dies im vereinbarten Leistungsumfang, über manuelle Eingaben, Uploads oder angebundene Schnittstellen vorgesehen ist,
- der technischen Administration,
- des Supports,
- der Fehleranalyse,
- der Datensicherung,
- der Bereitstellung von Reports oder Exporten, soweit vereinbart,
- der Durchführung vereinbarter Studien- oder Versorgungsprozesse.

4. Kategorien von Personendaten

Die Bearbeitung kann insbesondere folgende Kategorien von Personendaten umfassen (nachfolgend auch «Auftragsdaten»):

- Stammdaten von Patientinnen und Patienten,
- Kontaktdaten,
- Geburtsdatum,
- Geschlecht,
- Patientennummern oder interne Kennungen,
- Gesundheitsdaten,
- Diagnosen,
- Symptome,
- Schweregrade,
- Wohlbefinden,
- Vitalparameter,
- Gewicht,
- Blutdruck,
- Puls,
- Sauerstoffsättigung,
- Temperatur,
- Blutzucker,
- EKG-Daten, soweit genutzt,
- CRP-Werte, soweit genutzt,
- Labordaten und diagnostische Werte, soweit im jeweiligen Leistungsumfang vorgesehen,
- Laborbefunde, Laborparameter, Referenzbereiche, Zeitpunkte der Probenentnahme, Befundzeitpunkte und zugehörige Metadaten, soweit über Schnittstellen, manuelle Eingaben, Uploads oder verbundene Systeme verarbeitet,
- Genomik-, Molekularpathologie- und biomarkerbezogene Daten, soweit im jeweiligen Leistungsumfang vorgesehen,
- Formulardaten, strukturierte Eingabeformulare, medizinische Dokumentationsformulare und zugehörige Freigabe- oder Statusinformationen,
- Daten im Zusammenhang mit interdisziplinären medizinischen Besprechungen, fachlichen Konsilen und Boards, einschliesslich Fallzusammenfassungen, Fragestellungen, Empfehlungen, Entscheiden, Protokollen und zugehörigen medizinischen Angaben, soweit im jeweiligen Leistungsumfang vorgesehen,
- Register- und Studiendaten, einschliesslich registerbezogener Einschluss-, Verlaufs-, Ergebnis- und Dokumentationsdaten, soweit im jeweiligen Leistungsumfang vorgesehen,
- Medikation,
- Therapieereignisse,
- Nebenwirkungen,
- Fragebogenantworten,
- Mitteilungen,
- Behandlungs- oder Verlaufshinweise,
- studienbezogene Angaben,
- Gesundheitsstatus,
- technische Nutzungsdaten,
- Logdaten,
- Benutzer- und Berechtigungsdaten.

Die konkrete Datenbearbeitung richtet sich nach dem zwischen den Parteien vereinbarten Leistungsumfang, der Systemkonfiguration und allfälligen vereinbarten Schnittstellen.

5. Kategorien betroffener Personen

Betroffene Personen können insbesondere sein:

- Patientinnen und Patienten der Auftraggeberin,
- Studienteilnehmerinnen und Studienteilnehmer,
- Nutzerinnen und Nutzer der Auftraggeberin,
- medizinisches Fachpersonal,
- Pflegepersonal,
- Studienpersonal,
- administrative Mitarbeitende,
- technische Administratoren.

6. Dauer der Bearbeitung

Die Bearbeitung beginnt mit Eintritt der Rechtswirkungen des zwischen den Parteien bestehenden Grundverhältnisses (siehe dazu Ziff. 1) oder mit Beginn der Nutzung von medidux™, je nachdem, was früher eintritt.

Sie endet mit Beendigung der Rechtswirkungen des Grundverhältnisses, soweit keine gesetzlichen Aufbewahrungspflichten, berechtigten Interessen, Weisungen der Auftraggeberin oder technischen Übergangsfristen entgegenstehen.

7. Weisungen der Auftraggeberin

Die Auftragsbearbeiterin bearbeitet Auftragsdaten ausschliesslich gemäss den Weisungen der Auftraggeberin, soweit diese schriftlich oder elektronisch dokumentiert sind.

Als Weisungen gelten insbesondere:

- diese Vereinbarung,
- das Angebot / Auftragsformular sowie allfällige weitere Dokumente, die das grundsätzliche Rechtsverhältnis zwischen den Parteien regeln,
- die vereinbarte Systemkonfiguration,
- schriftliche oder elektronisch dokumentierte Weisungen der Auftraggeberin.

Die Auftragsbearbeiterin informiert die Auftraggeberin, wenn sie der Ansicht ist, dass eine Weisung gegen Datenschutzvorschriften verstösst. Eine umfassende rechtliche Prüfungspflicht der Auftragsbearbeiterin besteht nicht.

8. Pflichten der Auftraggeberin

Die Auftraggeberin stellt sicher, dass:

- die Datenbearbeitung rechtmässig ist,
- Patientinnen und Patienten angemessen informiert werden,
- erforderliche Einwilligungen eingeholt werden,

- eine allfällig erforderliche Entbindung vom Arztgeheimnis vorliegt,
- die Nutzung von medidux™ mit internen Vorgaben vereinbar ist,
- nur berechtigte Personen Zugriff erhalten,
- Berechtigungen korrekt vergeben und aktualisiert werden,
- Betroffenenrechte erfüllt werden,
- medizinische und rechtliche Dokumentationspflichten eingehalten werden.

Die Auftraggeberin ist verantwortlich für die Richtigkeit, Zulässigkeit und Rechtmässigkeit der von ihr, ihren Nutzern oder Patientinnen und Patienten eingegebenen Daten.

9. Pflichten der Auftragsbearbeiterin

Die Auftragsbearbeiterin verpflichtet sich:

- Auftragsdaten nur für die vereinbarten Zwecke zu bearbeiten,
- Auftragsdaten vertraulich zu behandeln,
- nur Personen Zugriff zu gewähren, die diesen für ihre Aufgaben benötigen,
- Personen mit Zugriff auf Auftragsdaten zur Vertraulichkeit zu verpflichten,
- angemessene technische und organisatorische Massnahmen umzusetzen,
- die Auftraggeberin bei Betroffenenrechten angemessen zu unterstützen,
- Datenschutzverletzungen unverzüglich zu melden,
- Unterauftragnehmer nur gemäss dieser Vereinbarung einzusetzen,
- Auftragsdaten nach Vertragsende gemäss Weisung zurückzugeben oder zu löschen, soweit keine gesetzlichen Pflichten entgegenstehen.

10. Vertraulichkeit

Die Auftragsbearbeiterin stellt sicher, dass alle Personen, die Zugriff auf Auftragsdaten haben, einer gesetzlichen oder vertraglichen Vertraulichkeitspflicht unterliegen.

Die Vertraulichkeitspflicht gilt auch nach Beendigung des Vertragsverhältnisses fort.

11. Ort der Datenbearbeitung

Die Speicherung der Auftragsdaten erfolgt grundsätzlich in der Schweiz, sofern nichts anderes vereinbart ist.

Eine Bearbeitung oder ein Zugriff aus Staaten ohne angemessenes Datenschutzniveau erfolgt nur, wenn die hierfür erforderlichen datenschutzrechtlichen Voraussetzungen erfüllt sind, insbesondere geeignete Garantien wie Standardvertragsklauseln oder gleichwertige Schutzmassnahmen.

12. Unterauftragnehmer

Die Auftragsbearbeiterin darf Unterauftragnehmer beiziehen, soweit dies zur Leistungserbringung erforderlich ist.

Die Auftragsbearbeiterin stellt sicher, dass Unterauftragnehmer vertraglich zu Datenschutz, Datensicherheit und Vertraulichkeit verpflichtet werden.

Die Auftraggeberin wird über wesentliche Änderungen der Unterauftragnehmer in geeigneter Form informiert.
Widerspricht die Auftraggeberin einem neuen Unterauftragnehmer aus wichtigem datenschutzrechtlichem Grund innert angemessener Frist, bemühen sich die Parteien um eine angemessene Lösung. Ist keine Lösung möglich, kann die Auftraggeberin den betroffenen Leistungsteil kündigen.

Die Auftragsbearbeiterin haftet für die Einhaltung der datenschutzrechtlichen Pflichten durch Unterauftragnehmer wie für eigenes Verhalten.

13. Technische und organisatorische Massnahmen

Die Auftragsbearbeiterin trifft angemessene technische und organisatorische Massnahmen zum Schutz der Auftragsdaten.

Diese Massnahmen betreffen insbesondere:

- Zugriffskontrolle,
- Zugangskontrolle,
- Benutzer- und Berechtigungsmanagement,
- Verschlüsselung, soweit angemessen,
- Protokollierung,
- Backup- und Wiederherstellungsprozesse,
- Schutz vor unbefugtem Zugriff,
- Vertraulichkeit,
- Integrität,
- Verfügbarkeit,
- Belastbarkeit der Systeme,
- Prozesse zur Erkennung und Behandlung von Sicherheitsvorfällen,
- sichere Datenübertragung,
- Trennung von Datenbeständen, soweit erforderlich,
- regelmässige Überprüfung und Verbesserung der Sicherheitsmassnahmen.

Die Auftragsbearbeiterin darf Sicherheitsmassnahmen anpassen, sofern das Sicherheitsniveau nicht wesentlich gesenkt wird.

14. Meldung von Datenschutzverletzungen

Die Auftragsbearbeiterin informiert die Auftraggeberin unverzüglich, wenn ihr eine Verletzung der Sicherheit bekannt wird, die zu einer unbeabsichtigten oder unrechtmässigen Vernichtung, einem Verlust, einer Veränderung, einer unbefugten Offenlegung oder einem unbefugten Zugriff auf Auftragsdaten führt.

Die Meldung enthält, soweit verfügbar:

- Art der Verletzung,
- betroffene Datenkategorien,
- betroffene Personengruppen,
- ungefähre Anzahl betroffener Personen,
- mögliche Folgen,
- getroffene oder vorgeschlagene Massnahmen,
- Kontaktstelle für Rückfragen.

Informationen können nachgereicht werden, soweit sie nicht sofort verfügbar sind.

15. Unterstützung bei der Geltendmachung von Betroffenenrechten

Wendet sich eine betroffene Person mit der Geltendmachung von Rechten direkt an die Auftragsbearbeiterin, leitet diese das Begehren an die Auftraggeberin weiter, soweit es sich auf Auftragsdaten bezieht.

Die Auftragsbearbeiterin unterstützt die Auftraggeberin angemessen bei der Bearbeitung von:

- Auskunftsbegehren,
- Berichtigungsbegehren,
- Löschbegehren,
- Einschränkungsbegehren,
- Herausgabebegehren,
- Widersprüchen,
- weiteren datenschutzrechtlichen Ansprüchen.

Aufwendungen können nach Aufwand verrechnet werden, soweit die Unterstützung nicht bereits im vereinbarten Leistungsumfang enthalten ist.

16. Unterstützung bei Datenschutzpflichten

Die Auftragsbearbeiterin unterstützt die Auftraggeberin angemessen bei:

- Datensicherheitsfragen,
- Datenschutzverletzungen,
- Datenschutz-Folgenabschätzungen,
- technischen Auskünften,
- Anfragen von Aufsichtsbehörden, soweit sie die Auftragsdaten betreffen.

Aufwendungen können nach Aufwand verrechnet werden, soweit gesetzlich zulässig und soweit die Unterstützung nicht bereits vertraglich enthalten ist.

17. Prüfrechte

Die Auftraggeberin hat das Recht, die Einhaltung dieser Vereinbarung in angemessenem Umfang zu prüfen. Die Parteien stimmen Zeitpunkt, Dauer, Umfang und Durchführung einer Prüfung vorgängig ab. Die Prüfung kann durch eine unabhängige, fachkundige und zur Vertraulichkeit verpflichtete externe Stelle erfolgen.

Die Prüfung darf den Betrieb der Auftragsbearbeiterin nicht unverhältnismässig beeinträchtigen. Die Kosten einer Prüfung trägt die Auftraggeberin, sofern die Prüfung keine wesentliche Vertragsverletzung der Auftragsbearbeiterin ergibt.

18. Rückgabe und Löschung nach Ende der vertraglichen Beziehungen

Nach Beendigung der vertraglichen Beziehungen, die sieser Vereinbarung zugrunde liegen, gibt die Auftragsbearbeiterin die Auftragsdaten auf Weisung der Auftraggeberin zurück oder löscht sie, soweit keine gesetzlichen Aufbewahrungspflichten oder sonstigen rechtlichen Gründe entgegenstehen.

Die Rückgabe erfolgt in einem gängigen Format, soweit technisch möglich und vertraglich geschuldet.

Die Auftragsbearbeiterin kann Sicherungskopien für eine technisch erforderliche Übergangszeit vorhalten, sofern diese angemessen geschützt sind und nach Ablauf der Frist gelöscht werden.

19. Nutzung anonymisierter oder aggregierter Daten

Die Auftragsbearbeiterin darf anonymisierte oder aggregierte Daten für folgende Zwecke verwenden:

- Qualitätssicherung,
- Produktverbesserung,
- Sicherheitsanalysen,
- statistische Auswertungen,
- technische Optimierung,
- regulatorische Nachweise,
- wissenschaftliche oder interne Auswertungen, soweit keine Re-Identifikation möglich ist.

Eine Nutzung ist nur zulässig, sofern keine Rückschlüsse auf einzelne Patientinnen und Patienten oder vertrauliche Informationen der Auftraggeberin möglich sind.

20. Haftung

Die Haftung der Parteien richtet sich nach den entsprechenden Regelungen, die auf das Grundverhältnis zwischen den Parteien Anwendung finden.

21. Schlussbestimmungen

Änderungen dieser Vereinbarung bedürfen der Schriftform oder einer von beiden Parteien akzeptierten elektronischen Form.

Sollten einzelne Bestimmungen unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Es gilt Schweizer Recht. Gerichtsstand ist Zürich.