Data Processing Agreement (DPA) medidux™

between

[Customer name]
[Address]
[Postcode, city]
Switzerland

hereinafter the “Customer”

and

mobile Health AG
Mühlebachstrasse 43
8008 Zurich
Switzerland

hereinafter the “Processor”

together, the “Parties”

Contents

1. Purpose of the Agreement 3
2. Roles of the Parties 3
3. Subject matter, nature and purpose of processing 3
4. Categories of personal data 4
5. Categories of data subjects 5
6. Duration of processing 5
7. Customer instructions 5
8. Customer obligations 5
9. Processor obligations 6
10. Confidentiality 6
11. Location of processing 6
12. Sub-processors 6
13. Technical and organisational measures 7
14. Notification of personal data breaches 7
15. Assistance with data subject rights 7
16. Assistance with data protection obligations 8
17. Audit rights 8
18. Return and deletion after the contractual relationship ends 8
19. Use of anonymised or aggregated data 8
20. Liability 9
21. Final provisions 9

1. Purpose of the Agreement

This Data Processing Agreement governs the rights and obligations of the Parties in connection with the Processor's processing of personal data on behalf of the Customer in relation to the use of medidux™.

It supplements the offer, the General Terms and Conditions / Terms of Use for medidux™ SaaS and any other agreements between the Parties.

If this Agreement contains provisions that differ from those in the documents listed above, this Agreement shall prevail.

2. Roles of the Parties

In connection with the use of medidux™, the Customer determines the purposes and means of processing patient and other personal data and is therefore the controller under data protection law.

The Processor processes personal data on behalf of and in accordance with the Customer's instructions, except where it exceptionally acts to meet its own legal obligations or in its own capacity as controller.

3. Subject matter, nature and purpose of processing

The subject matter of processing is the technical provision, storage, transmission, display, support, backup and evaluation of data in connection with the agreed use of medidux™.

Processing is carried out in particular for the purposes of:

- providing the medidux™ platform,
- structured collection of patient-related information,
- displaying symptom, vital sign, medication, progress, questionnaire, laboratory and diagnostic data,
- processing, displaying, transmitting and storing laboratory and diagnostic data where provided for in the agreed scope of services, through manual entries, uploads or connected interfaces,
- supporting communication and care by the Customer,
- processing, displaying, transmitting and storing genomics, molecular pathology, biomarker, form, registry, study, board and consultation data where provided for in the agreed scope of services, through manual entries, uploads or connected interfaces,
- technical administration,
- support,
- error analysis,
- data backup,
- providing reports or exports where agreed,
- conducting agreed study or care processes.

4. Categories of personal data

Processing may include in particular the following categories of personal data (also referred to as “Processed Data”):

- patient master data,
- contact details,
- date of birth,
- gender,
- patient numbers or internal identifiers,
- health data,
- diagnoses,
- symptoms,
- severity levels,
- wellbeing,
- vital signs,
- weight,
- blood pressure,
- pulse,
- oxygen saturation,
- temperature,
- blood glucose,
- ECG data, where used,
- CRP values, where used,
- laboratory data and diagnostic values where included in the relevant scope of services,
- laboratory findings, parameters, reference ranges, sample collection times, finding times and related metadata processed through interfaces, manual entries, uploads or connected systems,
- genomics, molecular pathology and biomarker data where included in the relevant scope of services,
- form data, structured input forms, medical documentation forms and related release or status information,
- data relating to interdisciplinary medical meetings, specialist consultations and boards, including case summaries, questions, recommendations, decisions, minutes and related medical information, where included in the relevant scope of services,
- registry and study data, including registry-related enrolment, progress, outcome and documentation data, where included in the relevant scope of services,
- medication,
- treatment events,
- side effects,
- questionnaire responses,
- communications,
- treatment or progress notes,
- study-related information,
- health status,
- technical usage data,
- log data,
- user and permission data.

The specific processing of data is determined by the scope of services agreed between the Parties, the system configuration and any agreed interfaces.

5. Categories of data subjects

Data subjects may include in particular:

- the Customer's patients,
- study participants,
- the Customer's users,
- healthcare professionals,
- nursing staff,
- study staff,
- administrative employees,
- technical administrators.

6. Duration of processing

Processing begins when the legal effects of the underlying relationship between the Parties take effect (see Section 1) or when use of medidux™ begins, whichever occurs first.

Processing ends when the underlying relationship ends, unless statutory retention obligations, legitimate interests, the Customer's instructions or technical transition periods require otherwise.

7. Customer instructions

The Processor processes Processed Data solely in accordance with the Customer's instructions, provided that they are documented in writing or electronically.

Instructions include in particular:

- this Agreement,
- the offer / order form and any other documents governing the underlying relationship between the Parties,
- the agreed system configuration,
- written or electronically documented instructions from the Customer.

The Processor shall inform the Customer if it considers an instruction to breach data protection requirements. The Processor has no general duty to conduct a comprehensive legal review.

8. Customer obligations

The Customer shall ensure that:

- processing is lawful,
- patients are adequately informed,
- required consents are obtained,
- any required waiver of medical confidentiality is in place,
- use of medidux™ complies with internal requirements,
- only authorised persons have access,
- permissions are correctly assigned and updated,
- data subject rights are fulfilled,
- medical and legal documentation obligations are met.

The Customer is responsible for the accuracy, permissibility and lawfulness of data entered by the Customer, its users or patients.

9. Processor obligations

The Processor undertakes to:

- process Processed Data only for the agreed purposes,
- keep Processed Data confidential,
- grant access only to persons who need it for their duties,
- require persons with access to Processed Data to maintain confidentiality,
- implement appropriate technical and organisational measures,
- reasonably assist the Customer with data subject rights,
- promptly report personal data breaches,
- engage sub-processors only in accordance with this Agreement,
- return or delete Processed Data after the contract ends, as instructed, unless legal obligations require otherwise.

10. Confidentiality

The Processor shall ensure that all persons with access to Processed Data are subject to a statutory or contractual duty of confidentiality.

The duty of confidentiality continues after the contractual relationship ends.

11. Location of processing

Processed Data are generally stored in Switzerland unless otherwise agreed.

Processing or access from countries without an adequate level of data protection is permitted only if the required data protection conditions are met, in particular appropriate safeguards such as standard contractual clauses or equivalent measures.

12. Sub-processors

The Processor may engage sub-processors where necessary to provide the services.

The Processor shall ensure that sub-processors are contractually bound to data protection, data security and confidentiality obligations.

The Customer will be notified appropriately of material changes to sub-processors.
If the Customer objects to a new sub-processor for an important data protection reason within a reasonable period, the Parties shall seek an appropriate solution. If no solution can be reached, the Customer may terminate the affected part of the services.

The Processor is liable for sub-processors' compliance with data protection obligations as if for its own conduct.

13. Technical and organisational measures

The Processor shall take appropriate technical and organisational measures to protect Processed Data.

These measures include in particular:

- access control,
- entry control,
- user and permission management,
- encryption, where appropriate,
- logging,
- backup and recovery processes,
- protection against unauthorised access,
- confidentiality,
- integrity,
- availability,
- system resilience,
- processes for detecting and handling security incidents,
- secure data transmission,
- separation of data sets where required,
- regular review and improvement of security measures.

The Processor may adjust security measures provided that the level of security is not materially reduced.

14. Notification of personal data breaches

The Processor shall notify the Customer without undue delay if it becomes aware of a security breach that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Processed Data.

Where available, the notification shall include:
• nature of the breach,
• categories of data affected,
• categories of persons affected,
• approximate number of persons affected,
• possible consequences,
• measures taken or proposed,
• contact point for follow-up questions.

Information may be provided later if it is not immediately available.

15. Assistance with data subject rights

If a data subject contacts the Processor directly to exercise rights, the Processor shall forward the request to the Customer insofar as it relates to Processed Data.

The Processor shall reasonably assist the Customer in handling:
• access requests,
• rectification requests,
• erasure requests,

• restriction requests,
• data disclosure requests,
• objections,
• other data protection claims.

Additional work may be charged according to time spent unless the assistance is already included in the agreed scope of services.

16. Assistance with data protection obligations

The Processor shall reasonably assist the Customer with:
• data security matters,
• personal data breaches,
• data protection impact assessments,
• technical information,
• requests from supervisory authorities insofar as they concern Processed Data.

Additional work may be charged according to time spent where legally permitted and unless the assistance is already included in the contract.

17. Audit rights

The Customer may audit compliance with this Agreement to a reasonable extent. The Parties shall agree in advance on the timing, duration, scope and conduct of an audit. An audit may be conducted by an independent, qualified external party bound by confidentiality.

An audit must not disproportionately disrupt the Processor's operations. The Customer shall bear the audit costs unless the audit establishes a material breach of contract by the Processor.

18. Return and deletion after the contractual relationship ends

After termination of the contractual relationship underlying this Agreement, the Processor shall, on the Customer's instructions, return or delete the Processed Data unless statutory retention obligations or other legal grounds prevent this.

Where technically possible and contractually required, the data shall be returned in a commonly used format.

The Processor may retain backup copies for a technically necessary transition period, provided they are adequately protected and deleted when that period expires.

19. Use of anonymised or aggregated data

The Processor may use anonymised or aggregated data for the following purposes:

- quality assurance,
- product improvement,
- security analyses,
- statistical analyses,
- technical optimisation,

- regulatory evidence,
- scientific or internal analyses where re-identification is not possible.

Such use is permitted only if it is not possible to draw conclusions about individual patients or confidential information of the Customer.

20. Liability

The Parties' liability is governed by the provisions applicable to the underlying relationship between them.

21. Final provisions

Amendments to this Agreement must be made in writing or in an electronic form accepted by both Parties.

If any provision is or becomes invalid, the validity of the remaining provisions shall not be affected.

Swiss law applies. The place of jurisdiction is Zurich.