Appendix 2: Joint Controllership Agreement / Contract on Joint Controllership Under Article 26 GDPR

1. Subject of the Contract

1.1 The parties have entered into a contract for services as offered to the Client (hereinafter referred to as the "Main Contract"). The collaboration between the parties based on the Main Contract, especially in relation to the collection of Patient Experiences through client-specific questions, may entail that the parties jointly determine the purposes and essential means of processing certain personal data of users of the Platform (hereinafter referred to as "User Data" or "Data Processing"). Therefore, in the sense of data protection law, the parties act as joint controllers within the meaning of Article 26 in conjunction with Article 4 No. 7 GDPR.

1.2 This contract constitutes an agreement under Article 26 of the General Data Protection Regulation (GDPR) to regulate the processing of personal data under joint controllership of the parties (the "**Agreement**").

1.3 This Agreement governs the data protection rights and obligations of the parties in the execution of the collaboration and, in particular, specifies the distribution and fulfillment of tasks and obligations under applicable data protection law (especially the GDPR) between the parties with respect to the Data Processing.

2. Subject, Purpose, Means, and Scope of Data Processing

2.1 The subject and purpose of the data processing under joint responsibility is the processing of User Data to capture Patient Experiences as specifically described in the Main Contract.

2.2 The data processing pertains to the following specified types of data and categories of affected persons and is carried out in accordance with the provisions contained in this Agreement as follows:

- Category of affected persons: Users of the Platform.
- Categories of processed data: User Data, which includes data queried and provided by users, including Basic Data (such as demographic data) and Health Data as defined by Art. 4 No. 15 GDPR, including information on medications used, medical devices, and patient experiences, and more
- Legal basis: Consent of the users according to Art. 6 para. 1 lit. a or Art. 9 para. 2 lit. a GDPR.

- Duration of data processing: The duration of collaboration for the collection of Patient Experiences through client-specific questions, corresponding to the duration of the Main Contract.

2.3 Determined by the Client within the scope of data processing under joint responsibility are:

- Purposes of processing,
- Duration of data processing,
- Categories of affected persons, and
- Type of User Data,

by specifying the reason for and the product for which and the duration for which user-specific questions should be asked.

2.4 Determined by XO Life within the scope of data processing under joint responsibility are:

- Purposes of processing that relate to the operation of the platform and are not determined by the Client,
- Type of data required for the setup of a user account on the Platform,
- Means of processing as far as the operation of the platform and data storage and transmission are concerned.

2.5 The parties agree that the data processing takes place exclusively in a Member State of the European Union (EU) or in a Contracting State of the European Economic Area (EEA). Any transfer to a third country must be coordinated between the parties and can generally only take place if the specific conditions of Art. 44 et seq. GDPR are met.

2.6 For clarification, it is noted that the parties are not jointly responsible but separately responsible where the data processing does not take place within the framework of this Agreement and is not for the execution of the Main Contract. This includes, in particular,

2.6.1 Processing of User Data by XO Life for its own purposes such as product improvements;

2.6.2 Processing of data of the user by XO Life within the framework of the Platform when the user has given their consent to this;

2.6.3 Processing of User Data by the Client for its own purposes following the transmission of the data to it by XO Life.

3. Phases of Data Processing/Responsibilities and Accountability

3.1 The responsibilities regarding data processing are divided between the parties according to the phases of data processing as follows:

3.1.1 Consent Collection and Data Collection: XO Life is responsible for obtaining the consent declarations and collecting the User Data.

3.1.2 Data Storage: XO Life is responsible for the storage of User Data, as far as it concerns the operation of the platform.

3.1.3 Data Modification and Deletion: XO Life is responsible for modifying and deleting User Data, restricting their processing, and their transfer according to Article 20 GDPR, as far as it concerns the operation of the platform.

3.1.4 Structuring, Pseudonymization, and Anonymization: XO Life is responsible for the structuring, pseudonymization, and anonymization of the data.

3.1.5 Data Transmission: XO Life is responsible for transmitting pseudonymized and anonymized data to the client.

Each party processes User Data within the framework of this agreement only under the provisions of this agreement and for the documented purposes. This does not apply to the extent that Union law or the national law applicable to the parties obliges the parties to process data. In such cases, the party is obliged to inform the other party about the data processing, as far as this is not legally prohibited.

3.2 The parties are independently responsible for ensuring that they can comply with all existing legal retention obligations concerning the data. They are required to make appropriate data backup arrangements for this purpose (notwithstanding corresponding regulations in this agreement), especially in the case of termination of the collaboration.

4. Informing the Affected Persons

4.1 XO Life ensures compliance with the obligations to provide information as per Articles 13 and 14 of the GDPR. XO Life will provide users with the necessary information during the registration process for the platform in a precise, transparent, understandable, and easily accessible form, using clear and simple language at no charge. XO Life will include in the information as per Articles 13 or 14 GDPR a note on the subsequent processing by the Client. The Client is responsible for providing all necessary information and is solely responsible for the accuracy and completeness of the information, as well as for ensuring that the information complies with data

protection regulations. The Client is also responsible for the accessibility of any linked privacy information.

4.2 XO Life will provide users with the essential contents of this agreement as required by Article 26(2) second subparagraph of the GDPR.

4.3 The information to be provided under this clause 4 must be published on the platform in a form that is easily and always accessible.

5. Fulfillment of Other Rights of the Data Subjects

5.1 XO Life is responsible for processing and responding to requests for the exercise of other rights of users ("Data Subject Rights") under Articles 15 et seq. of the GDPR.

5.2 Notwithstanding the provision in clause 5.1 of this agreement, the parties acknowledge that data subjects may approach either party to exercise their respective data subject rights. If a data subject approaches the Client with a request, the Client is obliged to immediately forward the request to XO Life.

5.3 The Client supports XO Life to the necessary extent in responding to requests from data subjects.

5.4 In the event of a data subject's request for deletion, clause 3.2 of this agreement applies accordingly.

6. Security of Processing

6.1 The parties ensure, within their respective areas of responsibility, the implementation of appropriate technical and organizational measures to comply with applicable laws protecting personal data (especially Article 32 of the GDPR).

6.2 Upon request of one party, the other party must demonstrate the technical and organizational measures it has implemented in its area of responsibility through appropriate documentation.

7. Engagement of Processors

7.1 Each party hereby grants the other party general authorization to engage processors regarding data processing for their respective areas of responsibility. Processors engaged by XO Life can be requested by the Client upon demand. Contractual relationships with service providers that involve the testing or maintenance of data processing procedures or systems, or other ancillary services, do not require approval,

even if access to data cannot be excluded, as long as appropriate arrangements have been made to protect the confidentiality of the data.

7.2 Each party will inform the other party about intended changes concerning the engagement or replacement of processors regarding data processing. The other party has the right to object to the engagement of a potential processor on a case-by-case basis. An objection must be raised for a significant, demonstrable reason. If the objection is not raised within 14 days after notification, the right to object to the respective engagement expires. If the other party raises an objection, the engaging party is entitled to terminate the main contract and this agreement with a notice period of one month.

7.3 The agreement with a processor must meet the requirements of Articles 28, 29 GDPR. If a processor located outside the EU is to be engaged, clause 2.5 of this agreement applies accordingly.

8. Procedure in Case of Data Protection Breaches

8.1 Each party is responsible for investigating and addressing all breaches of personal data protection in their respective area of responsibility as per Article 4 No. 12 GDPR, including fulfilling all corresponding notification obligations to the competent supervisory authority under Article 33 GDPR or to the affected persons under Article 34 GDPR.

8.2 The parties will immediately notify each other of any detected data protection breaches and cooperate in any notifications under Articles 33, 34 GDPR, as well as in investigating and remedying data protection breaches to the extent necessary and reasonable, especially by promptly providing each other with all relevant information in this context.

8.3 Before the party responsible under clause 8.1 makes a notification to a supervisory authority or an affected person as per clause 8.1 of this agreement, it will coordinate the approach with the other party, as far as and to the extent that this is necessary and feasible considering the notification deadline of Article 33(1) GDPR.

9. Other Joint and Mutual Obligations

9.1 Both parties are obligated to appoint a qualified and reliable data protection officer pursuant to Article 37 of the GDPR or other applicable data protection laws, as long as the legal requirements for such an appointment exist.

9.2 The parties must ensure that all personnel involved in data processing are contractually bound to maintain confidentiality concerning the data.

9.3 The parties will include the data processing activities in their respective records of processing activities as per Article 30(1) GDPR and note there that the processing is carried out under joint responsibility.

9.4 Both parties must inform each other immediately and fully if any errors or irregularities in data processing or violations of the provisions of this agreement or applicable data protection law (especially the GDPR) are detected.

9.5 The parties will each designate a permanent contact person and their deputy for all matters related to this agreement, the collaboration, and the data processing.

9.6 The parties will support each other in complying with the stipulations agreed in this agreement and the applicable legal data protection provisions (especially the GDPR) to the extent necessary and reasonable. This includes, in particular:

9.6.1 The obligation to assist each other in establishing and maintaining appropriate technical and organizational measures as per clause 6 of this agreement;

9.6.2 The obligation to support each other in any necessary data protection impact assessment and any consultations with the competent supervisory authority as required by Articles 35, 36 GDPR;

9.6.3 The obligation to assist each other in setting up and maintaining their respective records of processing activities;

9.6.4 The obligation to comply with legal documentation obligations and to provide each other with relevant documentation upon request.

9.7 The parties commit to documenting all facts, impacts, and measures related to this agreement, the collaboration, or the data processing.

10. Cooperation with Supervisory Authorities

10.1 The parties will immediately notify each other if a data protection supervisory authority contacts them in relation to this agreement, the collaboration, or the data processing.

10.2 The parties agree that they must generally comply with requests from competent data protection supervisory authorities, particularly in providing requested information and allowing for inspections. The parties will grant necessary access, information, and inspection rights to the competent data protection supervisory authorities within this framework.

10.3 Where possible, the parties will consult with each other before complying with any inquiries from competent data protection supervisory authorities or releasing information related to this agreement, the collaboration, and the data processing to such authorities.

11. Liability

11.1 The parties are liable to the affected persons according to legal regulations.

11.2 Internally, the parties indemnify each other from any liability to the extent that they each share responsibility for the cause triggering the liability. This also applies concerning any fines imposed on a party for violations of data protection regulations, provided that the party fined has first exhausted all legal remedies against the penalty notice. The party subject to the penalty must inform the other party immediately upon learning of a pending or ordered fine and allow it to participate in responding during the hearing and objection to the penalty notice. If a party remains partially or wholly burdened by a fine that does not correspond to its internal share of responsibility for the violation, the other party is obligated to indemnify it to the extent that the other party shares responsibility for the violation sanctioned by the fine. A right to indemnification exists only insofar as the affected party has given the other party an opportunity to comment on and assist in defending against the fine.

12. Final Provisions

12.1 The provisions of the main contract govern the duration and termination of this agreement.

12.2 In the event of contradictions between this agreement and other agreements between the parties, especially the main contract, the provisions of this agreement prevail.

12.3 Should any provisions of this agreement become invalid, unenforceable, or contain a gap, the remaining provisions shall remain unaffected. The parties commit to replacing an invalid or unenforceable provision with a legally permissible provision that most closely matches the purpose of the invalid or unenforceable provision and best meets the requirements of Article 26 GDPR. The second sentence applies correspondingly in the case of a gap.