Model clause for site contracts to regulate the relationship between Sponsor and Site in accordance with the requirements of the EU General Data Protection Regulation

Appendix to "8. regulation of the sponsor - trial site relationship in accordance with the requirements of the EU General Data Protection Regulation".

JOINT CONTROLLERSHIP AGREEMENT IN ACCORDANCE WITH ARTICLE 26 PARAGRAPH (1) SENTENCES 2, 3, PARAGRAPH (2) SENTENCE 1 GDPR

between

[Please insert the name and address of the sponsor][1]

- hereinafter referred to as "**Sponsor**" –

and

[Please insert the name and address of the site]

- hereinafter referred to as "**Site**" –

Hereinafter, the Sponsor and the Site will also be individually referred to as a "**Party**" and jointly as "**Parties**".

For any enquiries relating to this agreement, the Parties designate the following contacts who are knowledgeable in data protection law[2]:

Sponsor: [please provide the contact and the contact data of the person in charge]

and

Site: [please provide the contact and the contact data of the person in charge].

[1] Please consider carefully who shall be the controller, as defined in the GDPR, and who will be a party to this agreement.

[2] The parties should ensure to account for the fact that competencies may change within the parties' companies. For example, they could use generic email addresses of a department or contact data of contacts that are in charge of data protection within each organisation in the context of this project.

Preamble

The Sponsor desires to conduct the clinical trial [please insert the study title] (hereinafter referred to as "**Study**") which is the subject matter of this agreement. Details can be found in the protocol (Appendix). The Site shall support the Sponsor in the planning and conduct of the Study and has the requisite knowledge, experience and capabilities for the conduct of the Study.

The Parties will process personal data in the Study. In this context, the Parties are joint controllers, as defined in Art. 4 no. 7, 26 GDPR.

This joint controller agreement in accordance with Article 26 paragraph (1) sentences 2,3, paragraph (2) sentence 1 GDPR (hereinafter referred to as **"Agreement"**) sets out the rights and obligations of the Parties in the joint processing of personal data. This Agreement applies to all activities in which employees of the Parties or data processors commissioned by them process personal data for the controllers in the context of the Study. The Parties have jointly determined the means and purposes of the processing activities described in more detail below. Unless otherwise defined, the terms used in this Agreement shall have the meanings assigned to them in the GDPR.

1. Joint controllership

(1) Unless otherwise agreed below, each Party shall ensure compliance with the legal regulations, in particular the lawfulness of the processing activities carried out by it.

(2) In the context of their joint controllership, the Sponsor is responsible for processing the pseudonymised data that is collected for the purposes of the clinical trial in accordance with the protocol and forwarded to the Sponsor, for providing and ensuring the security (Articles 24, 32 GDPR) of the eCRF, for monitoring (monitoring, audit, cf. Section 5.1 of the main agreement) and for reviewing the proper conduct of the Study. This also includes the responsibility for a transmission path between the Site and the eCRF that complies with the requirements set out in Art. 32 GDPR.

(3) In the context of their joint controllership, the Site is responsible for processing personal data in connection with the conduct of the Study. This specifically includes collecting Study data, monitoring and documenting the reaction of patients to the drug being evaluated in the Study, processing the knowledge gained and forwarding it to the Sponsor by eCRF in pseudonymised form, as well as reporting adverse events to the Sponsor. This includes the responsibility for processing such information in compliance with Art. 32 GDPR until it is forwarded to the transmission path between the Site and the eCRF for which the Sponsor is responsible.

(4) All activities performed prior to signing the clinical trial agreement, which includes this Agreement, are not part of the Parties' joint controllership.

(5) Any activities performed following completion of the examinations set out in the protocol, submission of all completed electronic case report forms (eCRFs) and close-out of the Site, including the final data cleaning and locking of the trial database for the Site, are not part of the Parties' joint controllership. This includes, without limitation, the scientific analysis and the approval of the drug that is evaluated in the Study or archiving.

(6) The Sponsor will provide Site with the patient information sheet as well as the informed consent form that were approved by the ethics committee and prepared in accordance with the requirements of the GDPR concerning processing of personal data as required by the protocol. The Site will provide subject

data that is required based on the provisions of the protocol and the informed consent form to Sponsor in pseudonymised form. The Site is not obliged to review the informed consent form.

2. Informing data subjects

The Parties are required by law to provide data subjects with the information required according to Articles 13 and 14 GDPR, as well as the key content of this Agreement, in precise, transparent language that is understandable to laypersons and in easily accessible form free of charge. This information is part of the patient information sheet to be prepared by the Sponsor. The Parties agree that the Site shall provide the information provided by the Sponsor concerning the processing of personal data to patients upon collection of the personal data. The Site is not obliged to review the information provided by the Sponsor for compliance with the legal requirements.

3. Data subject rights

(1) Data subjects may assert the rights they are entitled to under Articles 15 to 22 GDPR vis-à-vis all Parties, with the Site being offered to them as their primary contact. Where a data subject asserts their data subject rights vis-à-vis the Sponsor, the Sponsor will generally refer to the patient information sheet provided to the data subject and to the Site which shall be the primary contact for compliance with data subject rights.

(2) Each Party shall support the other in complying with data subject rights, maintaining the pseudonymisation. The Parties shall provide the information that is required from their area of responsibility to each other as needed. Where possible, this shall be done in pseudonymised form using the Study-specific identification number.

(3) In all other respects, the Parties themselves are responsible for implementing and complying with data subject rights regarding the data processed by their organisations or their contractors.

(4) Where a request is made for the erasure of personal data in accordance with Art. 17 GDPR, the Parties shall notify each other prior to erasing any data. The other party has the right to object to the erasure for a legitimate reason, for example in cases where it has a legal obligation to retain data. Exceptions to the requirement to erase data may exist, in particular, in cases where the data subject revoked their consent, for example if the stored personal data is still required to determine the effects of the drug to be evaluated, to ensure that the legitimate interests of the data subject are not adversely affected, to comply with the obligation to present a complete authorisation dossier or to exercise or assert legal claims.

4. Irregularities, data breaches and doubts concerning the legitimacy

(1) The Parties shall notify each other without undue delay and comprehensively if they notice any error or irregularity concerning data protection law provisions when reviewing the processing activities performed under this Agreement.

(2) The Parties are responsible for the reporting and notification obligations vis-à-vis the regulatory authority and the persons affected by a personal data breach resulting from Articles 33, 34 GDPR in their respective area of responsibility (cf. Section 1). The Parties shall notify each other without

undue delay of reporting personal data breaches in the context of the clinical trial at issue to the regulatory authority and shall forward the information required to submit the report to the other Party without undue delay.

(3) The Parties have the right to refuse to provide or transfer any additional personal data to the other Party if and to the extent that there are any doubts concerning the legal basis for such provision or transfer. This situation may arise where changed legal or factual circumstances lead to a new legal assessment, such as the initial or changed requirement of a legal basis in accordance with Art. 44 et seqq. GDPR, or where the processing is not justified based on the informed consent form used. Such circumstances may also arise from regulatory or court orders or publications issued by the regulatory authorities. In the cases described in this paragraph, the Parties shall work towards a clarification of the legal basis and, as applicable, agree on a provision (legal basis) that most closely reflects the scientific objective.

5. Data protection impact assessments

The Parties shall ensure in their respective area of responsibility (cf. Section 1) that any required data protection impact assessments, as defined in Art. 35 GDPR, have been conducted. To the extent this is necessary, the Parties shall support each other in this context.[3]

6. Retention of documentation

Any documentation, as defined in Art. 5(2) GDPR, that can be used as proof of proper data processing shall be retained by each Party in accordance with the legal rights and obligations beyond the termination of the Agreement.

7. Confidentiality and data security

(1) The Parties shall ensure within their respective area of responsibility that all employees involved in the processing of data keep such data confidential in accordance with Articles 29 and 32 GDPR and Section 203 of the German Criminal Code, as well as, for foreign partners, a comparable confidentiality standard, for the duration of their work and following termination of their employment and that they will be placed under an obligation to maintain data secrecy and instructed in the data protection provisions relevant to them prior to starting their work.

(2) The Parties must independently ensure their compliance with all statutory retention obligations concerning the data. They shall take adequate data security precautions (Art. 32 et seqq. GDPR) for this purpose. This specifically applies if the collaboration is terminated.

(3) The implementation, default settings and operation of the data processing systems used must comply with the requirements of the GDPR and other regulations, in particular the principles of data protection by design and data protection by default, and require use of appropriate technical and organisational measures corresponding to the state of the art.

[3] Note: Where specific provisions are required for the conduct of data protection impact assessments, the Parties are free to supplement the Agreement as needed.

8. Processors

Where the Parties use data processors, they undertake to enter a contract in accordance with Art. 28 GDPR within the scope of this Agreement. Actions taken and processing activities performed by a Party's processors are attributable to the Party. The Party commissioning the processor shall ensure compliance with any additional requirements set out in Chapter 5 GDPR.

9. Records of processing activities

The Parties shall include the processing activities in their respective records of processing activities, as described in Art. 30(1) GDPR, also and with a note concerning the nature of the processing activity performed under joint or individual controllership.

10.[4] Term and termination

(1) This Joint Controllership Agreement shall be in effect for the duration of the conduct of the Study. The separate termination of this Agreement for convenience is excluded. This shall not affect the right to terminate this Agreement for good cause.

(2) The Parties may terminate the main agreement and this Agreement at any time without notice ("Termination for Good Cause") in the event of a serious or continued violation of data protection regulations or the provisions of this Agreement by the other Party. A serious violation specifically exists where a Party does not comply, or did not comply, with the obligations set out in this Agreement , in particular the technical and organisational measures agreed, to a significant extent.

11. Liability

(1) Art. 82 GDPR remains uneffected. This Agreement does not justify any additional claim of data subjects or other third parties or any joint liability of the Parties.

(2) In the internal relationship between the Parties, each Party is liable to the other for the damage caused by processing activities performed in its area of responsibility. This also applies to fines by analogy.

[4] Only necessary where the parties are not identical to those of the main agreement, otherwise this clause does not need to be included.

12.[5] Amendments; retention; severability; choice of law; and jurisdiction

(1) Amendments and additions to this Agreement and all its components – including any representations made by the contractor – require a written agreement and the specific reference that it is an amendment or addition to this Agreement. This also applies to a waiver of this formal requirement.

(2) The defence of right of retention, as defined in Section 273 of the German Civil Code (BGB), is excluded with respect to all data and the related data storage media provided to a Party by the other Party under this Agreement.

(3) In the event of any conflicts between this Agreement and the main agreement, the provisions of this Agreement concerning data protection shall prevail. If individual parts of this Agreement are invalid, this shall not affect the validity of the remaining provisions of the Agreement. The Parties agree that they will replace such parts with a valid provision that most closely reflects the intended purpose of the Parties. The same applies if there is a contractual gap in the Agreement.

(4) This Agreement shall be governed by German law under exclusion of the conflict of law principles.

(5) The place of jurisdiction for any dispute arising under this Agreement is–where permitted – the city where the registered office of the Site is located.

For the Site

_____ _____

(Place, date) (Signature)

For the Sponsor

_____ _____

(Place, date) (Signature)

[5]Only necessary where the parties are not identical to those of the main agreement, otherwise this clause does not need to be included.