# DATA SHARING AGREEMENT

# EuRRECa/EuRR-Bone

This document describes the minimum arrangements for data provision **by** **the Core Registry and e-REC**. It is to be used as the basis of agreements made about specific services with individual bodies.

**THE UNDERSIGNED**:

1. **Leids Universitair Medisch Centrum (LUMC),** having its registered office and principal place of business at Albinusdreef 2, 2333 ZA Leiden, the Netherlands, legally represented by H.B.M. Onstein, managing director division 2, hereinafter referred to as **“Supplier”**;

and

2. XXXXX,having its registered office and principal place of business at XXXXX, in XXXXX, legally represented by XXXXX, hereafter referred to as the **“Recipient”**

The foregoing entities are solely referred to as “**Party**” and collectively referred to as “**Parties**”.

**WHEREAS**:

1. The parties participating in the e-REC and/or the Core Registry own the rights to certain data and are willing to provide the Recipient with such data through Supplier for the purpose of executing the Research XXXXX (hereinafter: the **“Research”**) as set forth in **Annex 1**;
2. On behalf of these parties, Supplier enters into this Data Sharing Agreement with Recipient, to ensure adequate protection of the data;
3. With this agreement, the Parties aim to determine the terms and conditions upon which the Recipient agrees to conduct the Research and upon which the Supplier agrees to transfer the data.

Now, therefore, in consideration of their mutual promises to each other, hereinafter stated, the Parties agree as follows:

**Definitions**

1. “**Controller**”, “**Data subject**”, “**Personal data**”, **“Pseudonymised data”**, “**Processing**”, “**Processor**” and “**Supervisory authority/authority**” shall have the meaning as in the General Data Protection Regulation (EU) 2016/679 (hereinafter: “**GDPR**”).
2. **“Data”** means the data as identified in **Annex 1** which the Supplier will transfer to the Recipient. As far as the Data will contain Personal Data before the transfer they will be pseudonymised as described in **Appendix 2 to Annex 2.**
3. **“Confidential information”** means any proprietary information, know-how, data, or procedure related to the data and disclosed by Supplier to Recipient pursuant to its rights or obligations under this Agreement.

**Clause 1. The processing of Personal Data**

* 1. The Supplier will provide the Recipient with the Data in accordance with the terms of this Agreement. Parties are considered as Controller with regard to their own processing of the Personal Data for the purpose of the Research. If the Recipient is based in a country that is not within the European Union and the European Commission has not adopted and adequacy decision for that country, as outlined in <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>, the international data transfer addendum as set out in Annex 2 is hereby incorporated into this Agreement and the Recipient will act accordingly.
	2. Recipient shall implement appropriate technical and organizational measures to meet the requirements of this Agreement, with respect to the use of data, and shall manage and use the databases in accordance with this Agreement.
	3. The Supplier warrants and undertakes that:
1. the Personal Data have been collected, processed and transferred in accordance with the GDPR and additional national data protection laws;
2. the Data will only contain Pseudonymised data and no directly identifing Personal data;
3. it has obtained any regulatory or ethics approvals necessary to collect the Data and transfer the Data to the Recipient;
4. it has full authority to transfer the Data to the Recipient.
	1. The Recipient warrants and undertakes that:
5. the Personal data will be processed in accordance with this Agreement.
6. the Data will be used for the sole purpose of the Research in accordance with the permitted uses of the Data specified in the informed consent form of the Data subjects from whom the Data were collected;
7. Data will only be shared with a third party when that is necessary for the purpose of the Research, in which case Recipient will enter into an agreement with that third party that includes at least the terms stated in this agreement;
8. the Data will only be processed outside the European Economic Area when the processing is in accordance with this Agreement, specifically Annex 2;
9. appropriate technical and organisational measures are in place to protect the Personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected;
10. all Personal data will be treated strictly confidential and shall have in place procedures so that any third party it authorises to have access to the Personal data, including employees and (sub)Processors, will respect and maintain the confidentiality and security of the Personal data. Any person or organisation acting under the authority of the Recipient, including a (sub)Processor, shall be obligated to process the personal data only on instructions from the Recipient and in accordance with the permitted use under this Agreement. This provision does not apply to persons authorised or required by law or regulation to have access to the Personal data;
11. in the event a Data subject withdraws its consent or objects to the use of the Data, Recipient will – at the instruction of Supplier – immediately return or destroy the Data from that particular Data subject.

1.5 Under no circumstances will the identity of the Data subject, or any means to derive such identity, be provided to Recipient. Recipient shall not carry out any procedures with the Data (linking, comparison, processing) through which the identity of Data subject could be derived.

1.6 If either Party becomes aware of a Personal data breach, that Party shall promptly notify the other Party/ies. In such a case Parties will fully cooperate with each other to remedy the Personal data breach, fulfil the (statutory) notification obligations timely and cure the damages. A Personal data breach refers to: 1) a Personal data breach according to applicable law in the territory where the Data are treated, and 2) a Personal data breach as meant in articles 33 and 34 of the European General Data Protection Regulation.

**Clause 2. Confidentiality**

2.1 Confidential Information is the sole property of the Supplier and shall be used by the Recipient solely for the purpose of the Research. The Recipient agrees not to disclose Confidential Information to third parties without the consent of the Supplier and under an agreement by the third party to be bound by the obligations of this Clause 2. The Recipient shall safeguard Confidential Information with the same standard of care that is used with Recipient’s own confidential information, but in no event less than reasonable care.

* 1. The obligations under this Clause 2 shall not extend to any information:
* which is or becomes publicly available through no breach of this Agreement;
* which Recipient can demonstrate that it possessed free of any obligation of confidence prior to, or developed independently from, disclosure under this Agreement;
* which Recipient receives from a third party which is not legally prohibited from disclosing such information; or
* which Recipient is required by law to disclose.

2.3 The obligations of this Clause 2 shall survive this Agreement for a period of three (3) years after termination or expiration of this Agreement. Upon the request of the Supplier, the Recipient agrees to return the Confidential Information to the Supplier or destroy, at the option of the Supplier, all copies of Confidential Information; provided, however, that Recipient shall be entitled to retain one (1) copy of Confidential Information solely to ensure compliance with its rights and obligations hereunder.

**Clause 3. Ownership of data**

3.1 Agreements about the ownership of the data are included in the Data Access Policy: https://eurreca.net/data-access-process/.

**Clause 4. Publication**

4.1 If data from the Core Registry and e-REC are used for a report or publication without any statistical or clinical input from the Registry project team the use of data must be acknowledged along with a disclaimer. The current recommended text for use in publications is available on the website: https://eurreca.net/publication-plan/.

4.2 Personnel from the Registry PMT must be included as co-authors in any publication or report when statistical or clinical input and analysis has been required from the PMT. Submission for review must occur at least 30 days prior to the intended publication. A copy of published research based on data from the Core Registry and e-REC must be sent to the registry PMT.

 The non-publishing Party shall be entitled to make editorial comments and/or to recommend delay for up to ninety (90) days to enable patent applications to be filed or to remove or alter all reference to any of their own Results or background (therein) they consider to be of a confidential nature. If no objection is received in writing within the ninety (90) days period, the publishing Party will be free to publish the manuscript or other form of disclosure submitted to the non-publishing Party.

4.3 The disclaimer to be included in publications and reports based on data from the Core Registry and e-REC that have not, with prior agreement, involved any statistical or clinical input from the registry project team is available on the website <https://eurreca.net/publication-plan/>.

The source and data handling methods should be made clear in the ‘Methods’ section. The abstract should also include ‘EuRRECa’ or ‘EuRR-Bone’ and ‘Core Registry’ or ‘e-REC’ which would allow for searching for publications with these key words (as appropriate). Logos for inclusion in publications and reports are available on the EuRRECa website ([www.eurreca.net](http://www.eurreca.net)) and/or the EuRR-Bone website ([eurr-bone.com/](https://eurr-bone.com/)).

Data published in the Endo-ERN and ERN-BOND reports are in the public domain, but EuRRECa and EuRR-Bone (as appropriate) should be acknowledged as the source of the data and the disclaimer used.

**Clause 5. Representations and warranties**

5.1 Other than the warranties set out in section 1.3 the Data is provided by the Supplier to the Recipient without any warranties whatsoever, express or implied, including any warranties for merchantability or fitness for a particular purpose.

5.2 Nothing in this Agreement shall be construed as granting to Recipient, either expressly or by implication, any right or licence to the Data, under any patent, patent application, trade secret, know how, confidential information, trade or service mark, copyright, or other intellectual and/or industrial property rights Supplier possesses or may possess, nor any option to any such right or license.

**Clause 6. Liabilities and indemnification**

6.1 The Recipient assumes the risk of any damage, loss, or expense associated with or resulting from the conduct of the Analyses or Recipient’s use of the Data, unless such damage or loss is caused by the gross negligence or wilful misconduct of the Supplier.

6.2 The Recipient will indemnify and hold the Supplier, its directors or employees harmless against all claims of any kind whatsoever that may arise or result from the use of the Data.

6.3 The Supplier shall not be liable toward the Recipient for any claims, costs or damages that may result, directly or indirectly, out of Recipient’s use of the Data and/or Results, unless and to the extent that damage is caused by gross negligence and/or due to wilful misconduct by the Supplier.

6.4 The Parties shall in no case be liable for any indirect, incidental or consequential damages (including without limitation, lost business or profits, or loss of use of equipment) suffered by another party.

**Clause 7. Duration and termination of the Agreement**

7.1 This Agreement shall become effective on the date of the last Party’s signature below, and shall remain in force for the period of the Research, unless terminated earlier in accordance with section 7.2. The Parties agree that the term may be extended by mutual written agreement prior to expiry of the term.

7.2 This Agreement can be terminated earlier by either Party with immediate effect by receipt of written notice:

a. Upon a material breach of this Agreement by the other Party, if it is not cured within thirty (30) days after the breaching Party has received written notice of such material breach.

b. in the event the other Party is in state of bankruptcy or suspension of payment or a petition to that effect is filed by or against that Party;

c. in the event the business of the other Party will be winded up or closed down;

d. in case of force majeure - as determined in clause 11 below - if the force majeure situation will last over ninety (90) days.

7.3 The Recipient agrees, on termination of this Agreement (whether as a result of its breach or otherwise), to cease all use of the Data and shall within fifteen (15) days return all Data to Supplier or destroy all Data at the sole discretion of Supplier, or to deal immediately with the Data in accordance with Supplier’s written instructions. However, Recipient may retain one (1) copy of the Data solely for reproduction purposes.

7.4 Clauses 1-6, 8 and this section 7.4 shall survive expiration or early termination of this Agreement, as well as any terms that by their nature would be expected to survive expiration or early termination of this Agreement shall survive such expiration or early termination.

##### **Clause 8. Publicity**

##### Neither Party will use the logo or name of the other Party or the name of an employee of the other Party, for promotional purposes, in any publicity, advertising or news release, without prior written approval of the Party whose name is to be used.

##### **Clause 9. Modifications**

Modifications, changes and extensions to this Agreement are only binding after these have been agreed upon in writing between the Parties.

**Clause 10. Assignment**

 The rights and obligations as determined in the Agreement may not be assigned by a Party without the prior written consent of the other Party, which consent shall not be unreasonably with­held or delayed.

**Clause 11. Force Majeure**

In case of force majeure the concerning Party is entitled to suspend the obligations for the duration and extent of the force majeure, provided that the other Party has been notified in writing of the force majeure. Force majeure situations will concern those situations which prevent the execution of the Agreement and which are not imputable to the concerning Party pursuant to law, Agreement or according to generally accepted standards and as a result will not be attributable to that Party.

**Clause 12. Severability**

 The invalidity or unenforceability of any particular provision of this Agreement shall not affect any other provisions therein. The Agreement shall be construed in all respects as if such invalid or unen­forceable provision were omitted.

 **Clause 13. Governing law**

This Agreement shall be interpreted and governed by the laws of The Netherlands in any action. Any dispute relating to the interpretation or implementation of this Agreement which the Parties hereto have failed to settle amicably shall be exclusively referred to the competent courts of The Netherlands for settlement.

 **Clause 14. General Terms and conditions**

 No general conditions will apply to this Agreement.

**IN WITNESS WHEREOF**, the Parties hereto have by their authorized represen­tative duly caused this

Agreement to be executed as of the date hereinafter written.

**Leids Universitair Medisch Centrum XXXXXXXX**

……………………………………… ………………………………………

Date: …………………….… Date: …………………….…

Name: …………………….… Name: …………………….…

Title: …………………….… Title: …………………….…

**LUMC contact person / PI** **Recipient contact person / PI**

Name: Natasha Appelman-Dijkstra Name: ………………………

E-mail: N.M.Appelman-Dijkstra@lumc.nl E-mail: ..……….……..….….

**LUMC Data protection officer** **Recipient data protection officer**

E-mail: privacy@lumc.nl E-mail: ……………………..

**Annex 1: Protocol**

**Data request Form EuRRECa/EuRR-Bone**

[**https://link.webropolsurveys.com/Participation/Public/cf08917a-45b8-4c07-906c-bcec7d584ed0?displayId=Uni2326048**](https://link.webropolsurveys.com/Participation/Public/cf08917a-45b8-4c07-906c-bcec7d584ed0?displayId=Uni2326048)

**Shorter version to use:** [**https://link.webropol.com/s/eurreca-eurrbone-data-request-form**](https://link.webropol.com/s/eurreca-eurrbone-data-request-form)

**Annex 2: International data transfer addendum**

**STANDARD CONTRACTUAL CLAUSES**

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)([[1]](#footnote-1)) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter ‘entity/ies’) transferring the personal data, as listed in Annex I.A. (hereinafter each ‘data exporter’), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each ‘data importer’).

have agreed to these standard contractual clauses (hereinafter: ‘Clauses’).

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

**Third-party beneficiaries**

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.5 (e) and Clause 8.9(b);

(iv) Clause 12(a) and (d);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

**Interpretation**

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

**Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

**Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

**Docking clause**

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 8

**Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject’s prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation([[2]](#footnote-2)) of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter ‘personal data breach’). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter ‘sensitive data’), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union([[3]](#footnote-3)) (in the same country as the data importer or in another third country, hereinafter ‘onward transfer’) unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

[Intentionally left blank]

Clause 10

**Data subject rights**

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.([[4]](#footnote-4)) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter ‘automated decision’), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject’s rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject’s request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject’s request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11

**Redress**

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

• [OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body11 at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

**Liability**

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

**Supervision**

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

**Local laws and practices affecting compliance with the Clauses**

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards([[5]](#footnote-5));

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

**Obligations of the data importer in case of access by public authorities**

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

**Non-compliance with the Clauses and termination**

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

**Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

Clause 18

**Choice of forum and jurisdiction**

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Netherlands,

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Appendix

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

Appendix 1 to Annex 2

A. LIST OF PARTIES

**Data exporter(s):** *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: Leids Universitair Medish Centrum (LUMC)

Address: Albinusdreef 2, 2333 ZA Leiden, the Netherlands

Contact person’s name, position and contact details: ……

Data protection officer’s name and contact details: privacy@lumc.nl

Activities relevant to the data transferred under these Clauses: ……

Signature and date:

[SIGN & DATE]

Role (controller/processor): Controller

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

1. Name: ……

Address: ……

Contact person’s name, position and contact details: ……

Data protection officer’s name and contact details: ……

Activities relevant to the data transferred under these Clauses: ……

Signature and date:

[SIGN & DATE]

Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Patients with XXX, whose data is included in the Core Registry and e-REC.

Categories of personal data transferred

See data request form.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures

See data request form, but in any case health data, which will be pseudonymized and stored …

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

……

Nature of the processing

……

Purpose(s) of the data transfer and further processing

Conducting scientific research as described in the data request form.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

……

*Method of transfer*

Secured e-mail, e.g. Zivver or SURFfilesender.

*Authorized processors*

See data request form.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Autoriteit Persoonsgegevens (Dutch Data Protection Authority).

Appendix 2 to Annex 2

**TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

*Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*

*[Examples of possible measures:*

*• Measures of pseudonymisation and encryption of personal data*

*• Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services*

*• Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*

*• Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing*

*• Measures for user identification and authorisation*

*• Measures for the protection of data during transmission*

*• Measures for the protection of data during storage*

*• Measures for ensuring physical security of locations at which personal data are processed*

*• Measures for ensuring events logging*

*• Measures for ensuring system configuration, including default configuration*

*• Measures for internal IT and IT security governance and management*

*• Measures for certification/assurance of processes and products*

*• Measures for ensuring data minimisation*

*• Measures for ensuring data quality*

*• Measures for ensuring limited data retention*

*• Measures for ensuring accountability*

*• Measures for allowing data portability and ensuring erasure]*

1. () Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915. [↑](#footnote-ref-1)
2. () This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible. [↑](#footnote-ref-2)
3. () The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses. [↑](#footnote-ref-3)
4. () That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension. [↑](#footnote-ref-4)
5. () As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies. [↑](#footnote-ref-5)