Background information Joint Data Registry Agreement (JDRA)

This document governs:
The legal and organisational aspects of a collectively managed data collection with a centralised infrastructure

- in which health data of a given patient group are collected (entered by the **participating centres: in this document called Contributors)** and
- in which these data are also issued again (to the Contributors) for the purpose of scientific research.

Described is:

- What the data collection consists of
- The role the parties have in this collaboration
- The structure of the organization
- The way in which privacy is safeguarded
- Under what conditions the data will be provided

Further explanation of some Appendices:

- **The Contributors are joint controllers** with respect to the Registry. This is legally regulated in Annex C (joint controller terms and conditions).
- One of the Contributors (**the Coordinator**) manages the Database. In this role, **this Contributor is a data Processor**. To regulate this legally, Annex B has been added (**Processor terms and conditions).** The **Processor** enters into subprocessor agreements with hired subprocessors.
  The Coordinator has 2 roles:
  - the role of Processor in which he is instructed by the controllers to manage the Database, and
  - the role of Contributor (entering data into the Database and requesting them for scientific research).
- Accession to the Registry is done by signing Appendix D (by the authorized signatory of the Contributor). The legal department of the Contributor should review the document and determine whether accession to the registry is in accordance with the internal policy/rules of the Contributor. After the JDRA is made final, new Contributors can only join by accepting the unamended JDRA. Modification of the JDRA is possible only upon revision of the document by the Steering Committee (see revision date), after which the modified version is submitted to the Contributors' legal departments for agreement.
- The Coordinator will join the Registry by signing Appendix G.

Advantage:
This document avoids the need for contracts at each data entry and data release compared to a standard data sharing agreement.
Note: Data transfer to external parties that do not have a signed accession form still require a Data Sharing Agreement (by the Coordinator on behalf of the Contributors who are represented by the Steering Committee). For this purpose, we have a template DSA in place, which will be used when required.

EuRREB

Joint Data Registry Agreement

Version	2.0
Status	Definitive
Positive advice of LUMC privacy officer received on:	26 February 2026
Approved by	Registries Project Management Team
Steering Committee informed on:	8 February 2026
Date of Approval	10 March 2026
Revision date	10 March 2029

Contents

1.1 Definitions 4
1.2 Abbreviations 5
2. The Registries 6
3. Data collection and transfer to the EuRREB Registries 7
4. Governance 7
5. Privacy 9
6. Conditions for Data Access 10
7. Ownership and Intellectual property rights 12
8. Authorship 12
9. Accession 13
10. Finance 13
11. Subject complaints procedure 13
12. Limitation of liability 13
13. Duration and Termination 13
14. Confidentiality 14
15. Governing Laws 15
APPENDIX A: RESEARCH PROTOCOLS AND DOCUMENTATION COORDINATOR (AND AMENDMENTS) 16
APPENDIX B: DATA PROCESSOR TERMS (Coordinator) 17
ANNEX 1 TO APPENDIX B: TECHNICAL AND ORGANISATIONAL CONTROL MEASURES 21
APPENDIX C: JOINT CONTROLLER TERMS (Contributors) 22
APPENDIX D: MODEL ACCESSION FORM 28
APPENDIX E: MAIL OF APPROVAL FORMAT 28
APPENDIX F: FINANCIAL ARRANGEMENTS 31
APPENDIX G: DECLARATION OF ACCEPTANCE (Coordinator) 32
APPENDIX H: STANDARD CONTRACTUAL CLAUSES 33

1.1 Definitions

In this Joint Data Registry Agreement the following terms have the meanings as described below:

a) **Aggregated data**: refers to a summary and brief analysis of raw data that is not directly or indirectly identifiable.

b) **Confidential Information:** means any information, in tangible or non-tangible form, that is marked as confidential by the disclosing Party or that is clearly recognizable as confidential to a reasonable person with no special knowledge of the disclosing Party's activities. If Confidential Information is disclosed orally, the Confidential Information will be identified as confidential at the time of disclosure.

c) **Coordinator**: means the Contributor of the Registry who has been assigned this role. In this Registry, **Leiden University Medical Center (LUMC)** is the Coordinator.

d) **Contributor**: Each Contributor to the Registries that has signed the Accession form of this Joint Data Registry Agreement (attached hereto as **Appendix D)**.

e) **Controller:** means the natural or legal entity, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

f) **Data:** means the retrospective and prospective (raw) data collected from Subjects stored in the Registries in Pseudonymised form. For the purpose of this Joint Data Registry Agreement, Data are considered Personal Data.

g) **Database:** means the Registries Database containing the Data.

h) **Dataset:** means the Data from the Registries made available for the purpose of a Study.

i) **GDPR**: means the General Data Protection Regulation (EU) 2016/679.

j) **Joint Data Registry Agreement**: means this Agreement including its appendices and any future amendments to it.

k) **Personal Data:** means any information relating to a Subject; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

l) **Processor**: means the Contributor who processes the Data on behalf of the Controllers.

m) **Project Management Team**: the dedicated team of Coordinator that is dedicated to the daily handling of the database.

n) **Pseudonymised:** means the processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.

o) **Registry/Registries:** a collectively managed data collection with a centralised infrastructure in which health data from a particular patient group are collected and in which these data are also issued for scientific research purposes.

p) **Research:** any form of structured investigation that is performed to gain new knowledge or confirm previous findings.

q) **Researcher:** means any employee (or affiliated physician) of a Contributor Obtaining access to Data for Studies in accordance with this Joint Data Registry Agreement and Data Access Policy.

r) **Researcher's Institute**: means the Contributor employing (or otherwise engaging) the Researcher and which is liable for the activities of the Researcher in the context of this Joint Data Registry Agreement.

s) **Results:** means all results, know how, data, findings and information and all intellectual

property rights therein resulting from a specific Study.

t) **Study:** a research project of a Contributor within the Registries, using a Dataset, in accordance with a Study Proposal approved by the Data Access Committee.
u) **Study Proposal:** The document describing the scope, purposes, and methodology of a Study.
v) **Subject:** means any individual whose Data are transferred to the Registries in compliance with the terms and conditions of this Joint Data Registry Agreement.
w) **Third party**: means any entity other than a Contributor requesting access to Data.

1.2 Abbreviations

In this Joint Data Registry Agreement the following abbreviations have been used:

a) **2FA**: Two-Factor Authentication
b) **BOZ**: Dutch Healthcare Sector Associations (Brancheorganisaties Zorg)
c) **DAC**: Data Access Committee
d) **DPA**: Data Processing Agreement
e) **DPIA**: Data Protection Impact Assessment
f) **DSA**: Data Sharing Agreement
g) **DTA**: Data Transfer Agreement
h) **ECTS**: European Calcified Tissue Society
i) **EEA**: European Economic Area
j) **Endo-ERN**: European Reference Network on Rare Endocrine Conditions
k) **ERN**: European Reference Network
l) **ERN BOND**: European Reference Network on Rare Bone Diseases
m) **ESE**: European Society of Endocrinology
n) **ESPE**: European Society for Paediatric Endocrinology
o) **EU**: European Union
p) **EuRREB**: European Registries for Rare Endocrine and Bone Conditions
q) **FAIR**: Findable, Accessible, Interoperable, Reusable (data principles)
r) **GDPR**: General Data Protection Regulation
s) **IRB**: Institutional Review Board
t) **ISCBH**: International Society for Children's Bone Health
u) **ISO 27001**: ISO/IEC 27001 Information Security Management System Standard
v) **JDRA**: Joint Data Registry Agreement
w) **LUMC**: Leiden University Medical Center
x) **MD**: Medical Doctor
y) **NEN 7510**: Dutch Healthcare Information Security Standard
z) **NIST**: National Institute of Standards and Technology
aa) **PDF**: Portable Document Format
bb) **PMT**: Project Management Team
cc) **REC**: Research Ethics Committee
dd) **SC**: Steering Committee
ee) **SSL**: Secure Sockets Layer
ff) **UMCNL**: https://www.umcnl.nl/ University Medical Centers of the Netherlands
gg) **WGBO**: Dutch Medical Treatment Contracts Act (Wet op de Geneeskundige Behandelingsovereenkomst).

2. The Registries

1) **Background.** A core group of the European Reference Network on Rare Bone Diseases (ERN BOND) and Rare Endocrine Diseases (Endo-ERN) healthcare providers, patient representatives, affiliated centres and other experts, have joined their forces to address the need for standardised data collection on rare diseases by developing high-quality registries. Establishing a harmonised European Registry for Rare Endocrine and Bone conditions (EuRREB) will dramatically change this lack of high-quality and comprehensive data. The registries can improve the clinician-patient decision making, facilitate epidemiologic mapping, accelerate research, expedite validation studies, benchmark clinical outcomes, and provide leads for novel interventions. The registries consist of 2 platforms: e-REC and Core (the "Registries"). e-REC is a light touch registry only collecting the number new cases of a particular condition seen at a healthcare provider. It was designed to support the continuous monitoring of ERN's as well as to better understand and map the prevalence and incidence of certain conditions.
   The Core Registry requires patient informed consent and collects a very small amount of information for a wide range of rare conditions including those that are covered within the Endo-ERN and ERN BOND. The data collected in the Core Registry will be used to improve clinical care as well as research. Furthermore, the Core Registry allows the development of condition-specific modules which are collecting a condition-specific dataset making harmonised data collection throughout participating centres available.
   EuRREB is coordinated by the Leiden University Medical Center (LUMC), which hosts the central registry infrastructure and provides scientific, technical, and organisational support to participating centres.

2) **Main objectives**. The main objectives of the **Registries** are:
   (1) a secure FAIR (Findable, Accessible, Interoperable, Reusable) data infrastructure that can capture a core set of data for all patients and comprehensive data for a selection of diseases,
   (2) the means to engage patients in data provision,
   (3) the communication materials and efforts to connect healthcare providers and patients across Europe and beyond, and
   (4) maintain the open infrastructure for local initiatives and disease-specific registries to connect.

3) **Laws and Regulations**
   This Joint Data Registry Agreement is drafted taking into account EU law and regulations such as the EU General Data Protection Regulation. Notwithstanding, as the **Registries** are an international collaboration, the **Registries** also contain Data originating from countries outside the EEA, it is however not feasible to implement all national laws of the Contributors into this Joint Data Registry Agreement. All proceedings related to access and sharing must be compliant with European legislation. The processing of Data must be compliant with the provisions of the consent procedure and/or decision of an ethical review board, and/or a data protection authority/officer if applicable. It is the individual responsibility of each Contributor to ensure that no Data is entered into the **Registries** in violation of their own national law and legislation and that all Data can be used for the purposes of the **Registries**.

4) **Contributors outside the EEA**
   The **Registries** consist of Contributors within and outside the European Economic Area (EEA). Since section 5.3 of this Joint Data Registry Agreement identifies Contributors as Joint

Controllers in relation to the Data included in the Registry, the GDPR shall apply, whereby Contributors are considered Joint Controllers.
The Contributors will only process or transfer the Personal Data in or to countries outside the EEA under the conditions that the receiving Contributor has put in place appropriate safeguards, such as an Adequacy Decision or signing the Standard Contractual Clauses in accordance with the European Commission's decisions to ensure such transfer.

a. Adequacy Decision

For Contributors in countries with respect to which the European Commission has issued an Adequacy Decision, the following shall apply. When providing Data from the Database for the purpose of a Study to a Contributor in a country with an Adequacy Decision, the Processing of Personal Data for the purpose of the Study shall be in accordance with the national law of the Researcher to whom the data were provided.

b. Standard Contractual Clauses

Contributors outside the European Economic Area shall sign the Standard Contractual Clauses **(Appendix H**) (as data importer) with the Coordinator (as data exporter) before they receive data for the purpose of a Study.

3. Data collection and transfer to the EuRREB Registries

1) Each Contributor shall transfer into the **Registries**, Data of Subjects that consented to participate in the Core Registry and that are eligible to participate in the **Registries**. Consent shall be obtained in accordance with applicable national and European law for entering data in the Core Registry.

2) Transfer of Data into the **Registries** Database and the use of their own Data by the Contributors in accordance with this Joint Data Registry Agreement shall be free of charge. A fee for making available Data from the **Registries** to third parties (providing services) for the performance of analyses by the Contributors under Section 6.11 shall be determined by the Project Management team.

3) The Data in the **Registries** shall be used for research purposes only.

4) The Data provided is made available by the Contributors to support the research community. Each Contributor shall remain the owner of the source data it transfers into the **Registries**. Transfer of Data into the **Registries** shall not restrict any use of such Data by the Contributor that has contributed such Data.

5) It is the responsibility of each Contributor transferring Data into the Database, to ensure such transfer is in compliance with the law, including but not limited to privacy laws and that such Data can be used for the purposes of the **Registries**. If required, the **Registries Research Protocol** shall be submitted to a local review board, together with the informed consent forms and other relevant documents related to the **Registries** as determined by such review board.

6) Data shall be made available from the **Registries** by the Coordinator as a data Processor on behalf of the **Registries contributors** for Studies in accordance with **Section 6** hereof.

4. Governance

1) The objectives of the governance structure are to:
   - provide a sustainable infrastructure for standardized sharing of Data for specific and approved scientific research;

- ensure compliancy with the General Data Protection Regulation (EU) 2016/679 (hereinafter "GDPR") and with respect to Data originating from countries outside the European Economic Area, in accordance with such countries' privacy law provisions;
- monitor registry activities and supervise conduct of the **Registries**, taking all reasonable steps to ensure credibility and integrity of the Database;
- provide guidance for the review and approval of publications prior to submission;
- ensure that research outputs are prepared and curated in a way which helps maximise their value to the **Registries** Contributors;
- ensure that fair credit is given to the authors and to other individuals who have contributed significantly to the work that is described in each publication, report, or presentation.

2) The **Registries** have established a Project Management Team, a Steering Committee (SC), Data Access Committee (DAC), and Data Access Policy as can be found on the registries website: https://eurreb.eu/. The LUMC shall act as the Coordinator of **the Registries** in accordance with this **Section**.

The Steering Committee (see also https://eurreb.eu/steering-committee/) is chosen out of active contributors of the Registries and has representation of both ERNs, the major scientific societies within the field (ESPE, ESE, ECTS, ISCBH) and patient representatives. The Steering Committee has a remit after 4 years. Decisions by the Steering Committee shall be made by (qualified) majority as outlined in the Steering Committee remit **Appendix A** https://eurreb.eu/steering-committee/ The composition of the Registries Steering Committee is outlined in the Steering Committee Remit **Appendix A**. The Steering Committee will oversee the overall and financial management of the Registries on behalf of the Contributors. More specifically, the Steering Committee is authorised by the Contributors to and shall be responsible for:

- Governance and management regarding the Registries Data collection;
- To monitor progress of data sharing;
- To monitor the data sharing process;
- To select the network of investigators;
- To monitor progress of Study enrolment of centres;
- To monitor the data collection process;
- To ensure a scientifically sound and safe conduct of the Registries, eventually by executing an audit if desired;
- To address and resolve Study management problems;

3) The Coordinator and its Project Management Team is authorised by the Contributors to and shall be responsible for:
   - Making the Database available for the purpose of the **Registries**;
   - Governance and management regarding the **Registries** Database;
   - Maintaining, securing and hosting the **Registries** Database;
   - Processing the Data in the Database in accordance with the Research protocol, **Appendix A**, and this Joint Data Registry Agreement;
   - Concluding written agreements with new contributors and third parties providing services in relation to the Registries;

- Concluding written agreements with sub-contractors;
- Interacting with the subcontractors in maintenance and of central changes in the Database;
- Contact point for questions from Contributors regarding the organization of the Registries
- Contact point for questions related to Study Proposals;
- Adjustments of legal documents if appropriate;
- To review and approve the final Research Protocols and Amendments;
- To assist in the analyses and presentation of the Results;
- To assess Study Proposals

4) The Coordinator shall not be liable for any breach of contract .by a Contributor of a contract concluded by Coordinator pursuant to this **Section.**

5) Coordinator shall inform the Steering Committee of each signed JDRA with Contributors.

6) Pursuant to the decision-making procedures of the Registries as outlined in **Appendix A**, the Steering Committee may agree with the Coordinator on additional tasks.

7) The Data Access Committee shall be responsible for:
   - Promoting the wider use of the data that are being collected in the **Registries;**
   - Assessing and approving Study Proposals as described in Section 6.

5. Privacy

1) The Coordinator shall, as a data Processor, be responsible for maintaining and hosting the Database in accordance with the GDPR and any applicable national law of the Contributors it is informed of. The Coordinator shall act as a data Processor on behalf of the Joint Controllers (The Contributors) and shall process the Data in accordance with the terms set out in **Appendix B**. It is expressly agreed that none of the Parties shall carry out or attempt to carry out any procedures with the Data/Dataset - such as linking, comparison, or processing - with which the identity of the Subject could be derived.

2) Each Contributor is considered the Controller of its own Data up to the moment of transfer of such Data into the Database and shall fulfil all obligations of Controller under applicable privacy law.

3) In respect of the use of the Data for the purpose of creating and managing the Database, the Contributors are considered to be Joint Controllers. In view of article 26 of the GDPR, the privacy arrangements between the Contributors have been determined in the privacy matrix attached to this Agreement as **Appendix C**. In respect of the use of the Data for the purpose of performing a Study, the Contributor conducting the Study shall be a separate controller. In the case of several Contributors jointly performing the Study, they shall be Joint Controllers in accordance with Appendix C.

4) Contributors shall ensure that the privacy of the Subjects and the confidentiality of Data are protected in accordance with the statutory requirements applicable in their own country and the policies of the institute of which the Subject is a patient. The Coordinator shall not be responsible or liable for any failure of a Contributor to comply with national law and/or institutional policies with regard to the transferring of Data into the **Registries**.

5) Each Contributor shall use best efforts to ensure the accuracy of any Data that it enters into the Database and promptly to notify the Coordinator of any errors therein and, if so, instructed by the Coordinator, correct such errors.

6) Contributors shall transfer Data into the **Registries** in Pseudonymised form only, in accordance with the guidelines and instructions of the Project Management team. The key to coded Data is held at each Contributors own location for its own Subjects and is the responsibility of the local investigator who has collected the Data.

7) The Coordinator shall inform the Contributors about the method of Pseudonymisation and the location of the **Registries** (and any changes to the location).

8) Prior to making available the Data for a Study, the Dataset to be transferred shall be given a new pseudonym by the Coordinator.

6. Conditions for Data Access

Access by Contributors

1) Each Patient remains the owner of its Data in the **Registries** and is entitled to extract such Data from the Database for its own uses without the approval of the Data Access Committee. Each Contributor acts as a custodian of their patients data and is entitled to extract such Data from the Database for its own uses without the approval of the Data Access Committee. Furthermore, each Contributor shall be responsible and liable for the processing of its own Data in accordance with applicable laws.

Access by Researchers

2) Each Contributor shall be responsible for ensuring that Researchers, associated with their institute, shall be bound by this Joint Data Registry Agreement. The applicable conditions must be made known to the Researcher at least prior to the review of the Study Proposal.

3) Researchers requesting Data shall send their Study Proposal to the Coordinator who will submit this Proposal to the Data Access Committee in accordance with this Joint Data Registry Agreement. There is a preference for Researchers who are employees of or otherwise associated with a Contributor to submit a Study Proposal for Data release to the Coordinator but data can also be requested by others. If the Study includes the collaboration with a non-Contributor, the principal investigator of that Study proposal warrants that a separate contract for this collaboration shall be entered into, reflecting the relevant terms and conditions of this Joint Data Registry Agreement.
   If the requesting researcher is not associated with a Contributor and the other conditions of this section have been met, the Coordinator shall sign a Data Sharing Agreement that covers the terms of this Joint Data Registry Agreement with the organisation of that researcher.

4) Making Data available shall be conditional to having obtained approval from the Data Access Committee and to the extent applicable to any approvals, permits and licenses as required by the Researcher's national law.

5) If the Data Access Committee approves a Study Proposal, the Researcher will receive a 'Mail of Approval', as attached hereto as **Appendix E**, stipulating the general terms and conditions with regard to receipt and use of the Data. In order to have an overview of all Studies performed, all 'Approval emails' will be stored by the Coordinator.

6) The Researcher's Institute shall be considered a Controller under the GDPR in relation to the use of the Dataset for the purpose of the Study. The Mail of Approval may include provisions imposing on the Researcher (as representative of the Contributor additional obligations that the Contributor has as Controller under the GDPR). The Researcher then sends a confirmation email accepting the terms for use of the Dataset.

7) The Data Access Committee in its reasonable determination, may impose additional conditions on the performance of a specific Study. Such additional conditions will be communicated to the Researcher during the reviewing process and will be added to the Mail of Approval if the Study Proposal is approved.

8) Access to Data shall at least be conditional to the following:
   a) The Researcher's Institute shall be responsible for obtaining the permits and approvals necessary in its own country and required by its internal policies.
   b) The Researcher's Institute shall procure that Researcher shall use the Data for the approved Study only. In case of deviations or changes affecting the use of the Data in the Study the Project Management team in agreement with the Data Access Committee shall have the right to terminate the use of the Dataset for such Study without any liability at its sole discretion.
   c) The Researcher's Institute shall bear sole responsibility for the handling and use of the Data in accordance with applicable law and legislation and the additional obligations referred to in sections 6.6 and 6.7 of this Joint Data Registry Agreement.
   d) The Researcher's Institute shall procure that Researcher shall not duplicate the Data or have them duplicated unless in accordance with the approved Study proposal.
   e) Researcher's Institute shall procure that Researcher shall not disclose or provide access to the Data to any Third party without the prior written consent of the Project Management team. In case Data are sent to a Third party, a DTA must be concluded between that Party and the Coordinator.
   f) The Researcher shall report the progress of the Study and Results to the Coordinator in a manner and frequency as outlined in the Mail of Approval.
   g) Results must be shared with the research community at large and therefore be scientifically published in accordance with this Joint Data Registry Agreement and the registries publication guidelines as outlined on the Registries website in the publication guidelines https://eurreb.eu/obtaining-registry-data/

9) Researchers conditional to the above, shall have access to the Data free of charge unless specifically set forth otherwise in the Mail of Approval.

10) Upon receipt of the Mail of Approval on behalf of the Chairman of the Data Access Committee and – if applicable – the fee mentioned in the Mail of Approval, the dataset necessary to perform the Study will be selected from the **Database** and sent to the Researcher.

Commercial Use

11) Parties with commercial purposes will not be provided access to Data from the Registries for such commercial purposes. However, companies that make available funding may request certain analyses, based on an analysis plan developed by (a group of) Contributors in the form of investigator-initiated research, with reports and/or scientific publication as sole deliverable

in accordance with a separate funding agreement to be entered into between the Researcher's Institute and such Third party.

12) Parties with commercial purposes may be granted access to fully anonymised Aggregated data, subject to all Contributors involved in the approved Study proposal and any additional conditions determined by the Steering Committee in consultation with such Contributors. The Coordinator will ensure that the Dataset will have the characteristics of an Aggregated Dataset and then send it to the Third Party.

13) In no event shall Parties with commercial purposes own Results of such analysis as referred to in section 6.12.

7. Ownership and Intellectual property rights

1) The intellectual property rights as may apply to any Results of a Study, including but not limited to copyright in the resulting publications or algorithms, shall be owned by the Contributor(s) that employed the Researcher(s) or that generated the Results. The (other) Contributors shall have a non-exclusive right to use the Results for the purpose of further research in the field of rare endocrine, bone and mineral conditions and development of professional and/or medical standards.

2) If the possibility of commercial use of Results arises, the Contributors that generated the Results can develop an appropriate commercial strategy which strategy shall require prior assessment by and approval of the Steering Committee and the Project Management Team. When Results are used for commercial purposes by a Contributor or a Third party, but in the absence of an approved strategy, the Steering Committee and Project Management Team will come up with a proposal. The Coordinator shall act on behalf of the Contributors in the Steering Committee in its negotiations with the Contributor(s) or Third party involved.

8. Authorship

1. Authorship on Europe Outputs is based on the International Committee of Medical Journal Editors (ICMJE) as set out in: http://www.icmje.org/recommendations/browse/roles-and-responsibilities/defining-the-role-of-authors-and-contributors.html.

2. Authors: when a multi-author group has conducted the work, the investigators should decide who will be an author before the work is started and confirm who is an author before submitting the manuscript for publication. All members of the group named as authors should meet all four criteria for authorship: 1. Contributions to the conception, design, acquisition, analysis, or interpretation of the work 2. Drafting and revising the work 3. Approving the final version of the work prior to dissemination 4. Accountability for all aspects of the work.
   Contributors: those who meet fewer than all 4 of the above criteria for authorship should not be listed as authors, but acknowledged, either individually or as a group, and their contribution should be specified.
   Centres and reporters that have uploaded data into the Registries that has been used to conduct the study should be acknowledged as outlined on the Registries website in the publication guidelines https://eurreb.eu/obtaining-registry-data/

3. Researcher will enable the Project Management Team to review publications, including abstract before submission in accordance with any publication arrangements that are set out in the Mail of Approval sent to the Researcher. This review will be limited to potential issues with authorship (including author order), acknowledgement of contributors, and data protection and compliance, rather than a deep scientific review.

9. Accession

An entity becomes a Contributor to this Agreement upon signature of the accession document, attached as **Appendix D** to this Joint Data Registry Agreement, by the Coordinator and such entity. Such accession shall have effect from the date identified in the accession document. For sake of clarity, this accession will be notified to the Steering Committee.

10. Finance

Contributors will not be compensated for providing Data to the Registries, and the Coordinator will only be compensated for maintaining the Registries and the associated tasks. Any other financial arrangements should be disclosed in **Appendix F.**

11. Subject complaints procedure

Complaints of Subjects relating to or arising from the **Registries** shall be submitted to the institute of the Contributor at which the Subject is a patient and/or where Data were collected. The relevant Contributor warrants that the complaint shall be handled in accordance with the GDPR and **Appendix C**.

12. Limitation of liability

1) No Contributor shall be liable to any other Contributor for any loss or damages resulting from that Contributors participation to the Registries or its use of the Data, unless such loss or damage is caused by a breach of this Joint Data Registry Agreement or applicable law by that Contributor. In any event no Contributor shall be liable to any other Party for any indirect or consequential loss or similar damage such as, but not limited to, loss of profit, loss of revenue, loss of contracts or business opportunities.

2) The exclusions and limitations of liability stated above will not apply in the event the damage is caused by gross negligence or wilful misconduct of that Contributor and cannot be restricted or excluded by applicable law.

3) Each Contributor shall be solely liable for any loss, damage or injury to third parties resulting from the performance of said Contributors obligations under this Joint Data Registry Agreement or from its use of Data or Results unless such loss or damage is caused by a breach of this Joint Data Registry Agreement or applicable law by another Contributor.

4) Contributors receiving a claim based on (1) those Contributors being Joint Controllers, and (2) a breach of obligations under the GDPR by another Contributor, shall have recourse against said Contributor regarding any costs, damages and/or fines relating to such breach.

13. Duration and Termination

1) This Joint Data Registry Agreement shall come into effect on the date the Joint Data Registry Agreement has been approved by the Steering Committee (“Effective Date”) and shall continue

to be in effect until the Contributors determine that the **Registries** must be dissolved, in which case the Project Management Team shall prepare a proposal that includes at least transfer, destruction or return of the Data. If the Data are maintained in another Database after the **Registries** is dissolved, the proposal shall contain provisions for access and use of the Contributors and third parties. Any transfer of Data into another Database shall be in compliance with the terms of the GDPR. Upon termination, all Data shall be stored for an additional 10 years for verification purposes as required by applicable law and regulations, after expiration of which, the Coordinator shall delete such Data.

2) If any Contributor commits any breach of or is in default of any of the terms or conditions of this Joint Data Registry Agreement and fails to remedy such default or breach within thirty (30) days after the receipt of written notice from the Coordinator, the Coordinator may terminate the Participation of such Contributor to the Registries. Upon termination of the agreement, the data entered by the Contributor shall be deleted immediately from the database and archived for a period of two (2) years for verification purposes. If such breach is not remedied within that period or is not capable of remedy, the Steering Committee may furthermore declare the Contributor to be in default and to decide on the (legal) cause of action to be taken.

3) If a Contributor may terminate its participation in the Registries, it will inform the Coordinator of its intention. The withdrawing Contributor and the Coordinator shall in good faith discuss the consequences of such withdrawal. The foregoing provided that withdrawing Contributor shall continue to grant the user rights under this Agreement with respect to Data for the purpose of completing Studies approved prior to the termination date, after which the Data from the withdrawing Contributor in the Registries Database shall be destroyed or permanently de-identified. No additional Data will be entered into the Registries database by the Contributor after the effective date of withdrawal.

14. Confidentiality

Neither Party will disclose to any third party, or use for any purpose except carrying out the Research, any of the other Party's Confidential Information for a period of five (5) years after the initial disclosure of such Confidential Information, provided that the recipient Party's obligation shall not apply to information that:

a) was known to the receiving Party and not already subject to any obligation of confidentiality of the disclosing Party;

b) is or becomes generally known or publicly available without any breach of this Agreement;

c) has been obtained from a third party under no obligation of confidentiality;

d) has been independently developed by a Party;

e) is disclosed pursuant to the requirement of any law or regulation or the order of any court of competent jurisdiction; or

f) is approved for release in writing by an authorised representative of the other Party.

For the avoidance of doubt, if the Confidential Information contains Data, this will remain confidential indefinitely.

15. Governing Laws

Conflicts relating to this Joint Data Registry Agreement shall be governed by Dutch law and the Court of The Hague shall have exclusive jurisdiction. In deviation thereof, the Contributors shall be entitled to reach a different settlement with respect to conflicts that do not arise from the Registries.

APPENDIX A: RESEARCH PROTOCOLS AND DOCUMENTATION COORDINATOR (AND AMENDMENTS)

- **Original Grant applications:** available upon request (2018-2022 EuRRECa, 2020-2023 EuRR-Bone)
- **Ethics documents**: Approved protocols Coordinator, IRB approval, LUMC science committee regulations: https://eurreb.eu/ethics-approval/
- **Data Access Committee remit & Declarations of Interest:** https://eurreb.eu/data-access-committee/ **& Data Access Policy:** https://eurreb.eu/obtaining-registry-data/
- **Steering Committee remit & Declarations of Interest:** https://eurreb.eu/steering-committee/

APPENDIX B: DATA PROCESSOR TERMS (Coordinator)

Article 1. Background

Based on article 5.1 of the EuRREB Joint Data Registry Agreement, the Steering Committee has engaged the services of a data Processor to hold and maintain the Registries Database and the Data contained therein. The Data Processor is the Coordinator, LUMC.

Article 2. Definitions

2.1. In this Appendix B, capitalised terms shall have the meaning defined in the Joint Data Registry Agreement of the **Registries**. Additional capitalised words shall have the following meaning:

a.	Incident	i a complaint or request for information by a Subject with regard to the processing of Data by the Processor; ii an investigation or confiscation of Data by government officials or a suspicion that such may occur at some point in the future; and/or iii a personal data breach as meant in Article 4.12 of the GDPR.
b.	Sub-Processor	Any non-subordinate third party hired by the Processor to help process Data.
c.	Processor	The Processor within the meaning of Article 4.8 of the GDPR. The Steering Committee has designated the Coordinator as the Processor.
d.	Controller	Each Contributor making its Data available to the **Registries** and submitting it in the Database.

Article 3. The processing of the Data

3.1. The Processor shall only process Data on behalf of the Controller for the purposes outlined in the Joint Data Registry Agreement or as additionally agreed otherwise between the Processor and the Steering Committee.

3.2. Without prejudice to the provisions of Article 3.1, the Processor shall be allowed to process Data if it is required to do so by a statutory provision (including the court order or administrative decisions based on it). In such cases, the Processor shall to the extent permitted by law, notify the relevant Controller(s) of the intended processing of the Data and of the statutory provision prior to the processing. Processor shall minimise the extent of the enforced processing to the maximum extent possible.

3.3. The Processor shall process the Data in a proper manner, in accordance with the requirements to which it is subject under the GDPR and to the extent known to the Processor, the national privacy law of the Contributors.

3.4. In processing the Data, the Processor shall reasonably ensure that its procedures shall not violate health care legislation.

Article 4. The security and monitoring of Data

4.1. To protect the Data from loss, unauthorised inspection, damage or any other form of unlawful processing, and to guarantee the availability of the Data when due, the Processor shall implement appropriate and effective technological and organisational measures, which, considering the current state of the art and the costs associated with it, shall be in accordance with the nature of the Data to be processed. These security measures shall include the following:

a.) measures designed to guarantee that only authorised employees can access the Data for the purposes outlined;

b.) measures involving the Processor only granting its employees and Sub-Processors access to Data through individual named accounts, with the use of said accounts being adequately logged and with the accounts concerned only granting their users access to those Data whose access is necessary for the legal person concerned;

c.) measures designed to protect the Data from unintentional or unlawful destruction, unintentional loss, or changes and unauthorised or unlawful retention, processing, access or disclosure;

d.) measures designed to identify weaknesses with regard to the processing of Data in the systems used to provide services to the Controller(s);

e.) measures designed to guarantee that Data are separated in a sensible manner from the Data the Processor processes on its own behalf or on third parties' behalf;

f.) other measures agreed between the Controller(s) and the Processor [Optional: in the Annex to this Appendix B].

4.2. The Processor's security measures shall comply with the requirements of the GDPR. Furthermore, the Processor has implemented an appropriate, written security policy for the processing of the Data.

4.3. Upon the request of a Contributor and provided that such certificate is in place, the Processor shall submit a certificate issued by an independent and competent third party that shows that the Processor's methods comply with the requirements arising from this article 4.

4.4. Each Contributor is entitled to monitor (or have monitored) the Processor's compliance with this article 4 and shall enable such Contributor to inspect the Processor's processing methods, but no more frequent than once per year, unless such Contributor has reasonable doubts that the Data are not processed in accordance with the Joint Data Registry Agreement, this or applicable law.

4.5. If, in response to such inspection, the Contributor reasonably instructs the Processor to adjust or update its security policy, the Processor shall reasonably comply.

4.6. The Processor shall ensure that persons authorised to process the Personal Data on its behalf, have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality

Article 5. Monitoring, obligation to provide information and incident management

5.1. When an Incident occurs, has occurred, or may be about to occur, the Processor shall to the extent reasonably possible, undertake the activities necessary to undo the damage caused by the Incident as soon as possible or minimise the consequences to the maximum extent possible.

5.2. In addition, the Processor shall notify the relevant Controller(s) without undue delay and to provide any relevant information on:

a.) the nature of the Incident;
b.) the Data that (may) have been affected;
c.) the actual and likely consequences of the Incident; and
d.) the measures which have been or will be taken to resolve the Incident or to minimise the consequences or damage to the maximum extent possible.

5.3. The Processor shall consult the relevant Controller(s) on further arrangements to be undertaken with respect to the Incident and to prevent future Incidents.

5.4. The Processor shall cooperate with the relevant Controller (s) any time, shall follow the reasonable instructions of the relevant Controller (s) and shall enable the relevant Controller (s) to conduct an appropriate investigation of the Incident, formulate a response to the Incident and take appropriate subsequent steps, including notifying the Dutch Data Protection Authority and/or the Subject.

5.5. The Processor shall at all times have written procedural guidelines in place covering the handling of Incidents and shall furnish the relevant Controller (s) with a copy of such procedural guidelines upon the request.

5.6. Alerts under this article 5 shall be addressed to chair of the relevant Controller (s) or any other designee indicated by the relevant Controller (s).

5.7. The Processor shall not provide third parties any information on Incidents, except in cases where the Processor is legally required to do so or the Parties have otherwise agreed.

Article 6. Obligation of cooperation

6.1. The Processor shall fully cooperate with the relevant Controller(s) to enable and the relevant Controller (s) to fulfil their obligations under the GDPR. The Processor and relevant Controller (s) shall agree on procedures to comply with the rights of Subjects under the GDPR.

Article 7. The hiring of Sub-Processors

7.1. The Processor shall not outsource the processing of Data to a Sub-Processor without prior written permission from the Controller(s). The foregoing does not apply to the Sub-Processors listed in Appendix C.

7.2. If the Controller agrees to the hiring of a Sub-Processor, the Processor will enter into a processor agreement with the subprocessor based on the BOZ (Dutch Healthcare Sector

Associations) template. The Processor shall remain fully responsible for the processing of the Data by the Sub-Processor as if it has performed the processing itself.

7.3. The Processor shall not transfer any Personal Data to a country outside the European Economic Area (EEA), unless the Controller has expressly authorized such transfer in writing.

Article 8. Duration and termination

8.1. This Appendix B shall enter into force on the effective date of the Joint Data Registry Agreement and terminate upon termination of the **Registries** or so much earlier as foreseen in the Joint Data Registry Agreement or this Appendix B.

8.2. Obligations which, by their very nature, are meant to continue to apply even after the termination of this Appendix B shall continue to apply after the termination of this Appendix B. Such provisions shall include those which arise from provisions governing confidentiality, liability, dispute resolution and applicable law.

8.3. Upon expiration of the initial term of the **Registries** or upon earlier termination in accordance with the Joint Data Registry Agreement, the Processor shall discuss with the Steering Committee the feasibility and possibility of continuing the **Registries** or to destroy the Data.

Article 9. Retention period, restoration, and destruction of Data

9.1. The Processor shall not retain the Data longer than strictly necessary for the **Registries** and applicable law.

Article 10. Intellectual property rights

10.1. If the (collection of) Data is protected by any intellectual property rights, the Processor is herewith granted permission to process the Data as foreseen in the Joint Data Registry Agreement.

ANNEX 1 TO APPENDIX B: TECHNICAL AND ORGANISATIONAL CONTROL MEASURES

The Coordinator, LUMC, sees Data Security as an integral part of the processes within the organization. This is implemented by appropriate technical and organizational measures where necessary throughout the entire organization. Data are processed under our NEN7510 certified information security system. NEN7510 is the Dutch equivalent of ISO27001/2 with special additions for health care data.

Technical measures.

The technical measures include:

- Physical measures for access security, including organizational control
- Measures against malicious software (anti-virus, anti-spam, etc.)
- Safe for storing data files
- Logical access control using passwords or key authentication and 2-factor authentication
- Outer perimeter security through Next Generation Firewalls
- Securing network connections via SSL (Secure Socket Layer)
- Encryption by encryption of personal data during transmission

Organizational measures

The organizational measures include:

- Responsibilities for information security have been assigned
- Established security policy including implementation
- Employee confidentiality obligations
- Screening of new employees
- Change Management procedures for changes in data or in information processing
- Powers are granted based on the "Need-to-know" principle
- Periodic internal audits to ensure compliance with standards and requirements
- Periodic external audits to ensure compliance with standards and requirements
- Mandatory awareness training for employees with regard to security and privacy

APPENDIX C: JOINT CONTROLLER TERMS (Contributors)

Part I: Description of the Data

Data subjects The Personal Data transferred concern the following categories of data subjects:	Patients with the conditions listed in the Registries condition data dictionaries.
Purposes of contribution of Data The Data is contributed for the following purpose	The Data is contributed for the purposes of the Registries, which aims to collect, maintain and make available for research purposes data on patients with Rare Endocrine, Bone and Mineral conditions.
Categories of data The Personal Data transferred concern the following categories of data:	• Personal (demographic) • Sensitive data (health, ethnic and genetic)
Sensitive data The Personal Data contributed concern the following categories of sensitive data:	• Personal data: date of birth, sex at birth, current gender, country of birth and usual residence • Health data: collected as part of routine clinical care, e.g. anthropometric data, diagnostic data such as imaging, biochemistry, histology, therapy • Genetic data: WES analysis; WGS analysis, etc. See also the Core Registry protocol.
Method of transfer	Data is pseudonymised and processed to include only necessary variables. Data is sent encrypted via Zivver after DAC study approval, and a JDRA/DSA is signed with researcher's institute. Two-factor authentication (2FA) and reCAPTCHA to access interface.
Method of data storage and security measures (e.g. method of encoding)	The Registries Database is compliant with GCP, GDPR, and 21 CRF Part 11. It is located in a secure and fully certified data centre in the Netherlands. The Registries Database is certified to store medical

	data (NEN7510, ISO 9001 and 27001:2017). Data will be entered encoded and will be stored encrypted; the key to coded information is held at each Contributor for its own Subjects and is the responsibility of the local investigator. Handling of Personal Data by the Registries Database is in compliance with the GDPR.
Authorized sub-processors Identified at the Effective Date	None

Part II: Privacy arrangements **The Contributors are Joint Controllers with regard to the Personal Data that will be processed by virtue of the Registries. In this context Parties determine and agree on- in accordance with article 26 of the GDPR- their respective obligations with regard to compliance with the GDPR.**	
Privacy obligation (*please mention below the applicable privacy obligations).*	*Please mention below with regard to each obligation: the name of the responsible Party, the Personal Data and processing activities involved and if necessary, the arrangement(s) about how to fulfil the obligation.*
1. Provide information on the processing of the Personal Data to data subjects in accordance with article 13, 14 GDPR, The Medical Treatment Contracts Act (WGBO).	Each Contributor is responsible for providing information on the processing of Personal Data to the Subject in accordance with the GDPR.
2. Safeguarding that informed consent for the processing of the Personal Data is obtained or that another legitimate basis for the processing of the Personal Data is in place (article 6 and 9 GDPR).	Each Contributor is responsible that informed consent from Subjects is obtained and filed. These filed data may be subject to monitoring purposes.
3. Safeguarding that the data subjects can exercise their right of access, to rectification, erasure, restriction of processing and to object to the processing (articles 15 to 18 and article 21 GDPR).	If a Subject exercises any of its rights mentioned in the GDPR, the first addressed Contributor shall discuss with the Coordinator on the manner to safeguard the Subject's rights in accordance with the GDPR and the Dutch GDPR Implementation Act. N.B. the right of access, rectification and restriction of processing is exempted in

	Article 44 of the Dutch GDPR Implementation Act: "Where processing is carried out by institutions or services for purposes of scientific research or statistics, and the necessary steps have been taken to ensure that the personal data can be used solely for statistical or scientific purposes, the controller may refrain from applying Articles 15, 16 and 18 of the Regulation."
4. Safeguarding that the data subjects can exercise their right to data portability (article 20 GDPR),	Each Contributor shall include a local contact person in the patient information brochure whom the Subject can contact.
5. Safeguarding that the data subjects can exercise their right to object to the processing (article 21 GDPR)	Each Contributor is responsible for giving Subjects the opportunity to object to the processing of the data.
6. Safeguarding the security of the Personal Data in accordance with article 32 GDPR and in accordance with other arrangements in this Agreement.	Each Contributor is responsible for the safeguarding of the Personal Data in accordance with article 32 GDPR for its locally stored data. Each service provider, research party and other parties who might get access to the data of other parties are responsible for safeguarding the transfer of data, data monitoring, data cleaning and data analysis. The Coordinator is responsible for maintaining the Registries Database. The Database is compliant with GCP and GDPR. It is located in a secure and fully certified data centre in the Netherlands. The Registries Database is certified to store medical data (NEN7510, ISO 9001 and 27001:2013). Data will be entered encoded; the key to coded information is held at each Contributor for its own Subjects and is the responsibility of the local investigator. Handling of Personal Data by the Registries Database is in compliance with the GDPR.

	Each Contributor is responsible for correct Data input, their login accounts and local master files.
7. Comply with data breach obligations (articles 33 and 34 GDPR).	The Coordinator, Contributors and their Researchers shall comply with data breach obligations. If the Coordinator or any other Party identifies such a Data Breach within its sphere of control (Identifying Party), the Identifying Party: A. inform the Coordinator and the Party that provided the Dataset without undue delay, though not later than twenty-four (24) hours after discovering the Data Leak, about the nature of the Data Leak, the possible impact of the Data Leak on the Providing Party, and/or the Data Subject(s), and also about measures Identifying Party has taken or will take in order to correct the security breach and/or limit its consequences; B. will immediately, at its own expense, take all measures to correct the shortcomings in security that resulted in the Data Leak and to limit its consequences; C. will work together with the Providing Party to investigate the cause of the Data Leak and take all measures that Providing Party deems necessary to prevent a similar incident; and D. will grant full cooperation in timely (within forty-eight (48) hours) and adequately informing the Dutch Data Protection Authority ('Autoriteit Persoonsgegevens') and, if necessary, the Data Subjects (e.g., patients) within the framework of the obligation to report Data Leaks; Data Protection Officer of the Coordinator is: Data Protection Officer Leiden University Medical Center, Email: privacy@lumc.nl

8. Safeguarding that employees who have access to Personal Data are instructed by a binding agreement in accordance with Article 32 lid 4 GDPR, to process the Personal Data in conformity with the instructions of de Controllers to the Personal Data, including observing the duty of confidentiality with regard to the Personal Data.	All personnel involved in the registration and processing of the Data are registered as such in the delegation log form per Contributor. The Contributor is responsible for the accuracy of the log form, which is kept in the local master file by the local investigator. Contributor and Coordinator will safeguard that employees who have access to Personal Data are instructed by a binding agreement in accordance with Article 32 lid 4 GDPR, to process the Personal Data in conformity with the instructions of the controllers to the Personal Data, including observing the duty of confidentiality with regard to the Personal Data.
9. Safeguarding that engaged (sub) Processors who have access to Personal Data are instructed by a binding agreement (data Processor agreement) to process the Personal Data in accordance with the requirements stated in article 28 of the GDPR, including among others the documented instruction of the Controllers to the Personal Data and all other GDPR requirements applicable to the Processor.	The Coordinator is responsible for the security level of the Registries Database. The Coordinator will safeguard that engaged (sub) Processors who have access to Personal Data are instructed by a binding agreement (data Processor agreement) to process the Data in accordance with the requirements stated in article 28 of the GDPR, including among others the documented instruction of the Controllers to the Personal Data and all other GDPR requirements applicable to the Processor.
10. Safeguarding that: (1) regular monitoring takes place in order to assess if the processing of the Personal Data by the (sub) Processor is in compliance with the data Processor agreement entered into with the (sub) Processor; and (2) that breach of the data Processor agreement is addressed by appropriate measures.	The Coordinator together with the Steering Committee is responsible for monitoring any sub-processors and following up on any breaches by the sub-processors.
11. Safeguarding that the transfer of Personal Data takes place in accordance with the transfer requirements of the GDPR.	The Coordinator, Researcher and other parties who might get access to the data of other parties are responsible for the safeguarding that the transfer of Personal Data takes place

	in accordance with the transfer requirements of the GDPR. A Contributor may only transfer the Data outside the European Economic Area, provided that the following conditions are met 1) the Data Access Committee and Project Management Team have approved such transfer 2) the Coordinator has put in place appropriate safeguards such as signing the Standard Contractual Clauses in accordance with decisions by the European Commission to safeguards such transfer (to the extent the importer is located in a country outside the EEA for which no adequacy decision is in place), 3) such Third parties are only allowed to process Data in accordance with the Joint Data Registry Agreement, 4) Coordinator will on request provide information about the Third party, where Data is transferred to, including copies of safeguards that is governing such transfer 5) Subjects have been adequately informed of such transfer; 6) only pseudonymized data or aggregated data will be shared and 7) the Contributor will carry out a Data Transfer Impact Assessment (DTIA).
12. Safeguarding the compliance with the requirements regarding retention periods, destruction, return and/or migration of the Personal Data.	All source data will be kept for a period of 10 years after termination of the registry, as will be the eCRFs.
13. Safeguarding that a Privacy Impact Assessment (PIA) is executed prior to the collection, including obtaining and further processing of the Personal Data (Article 35 AVG).	A registry wide DPIA has been performed in collaboration with the DPO of the Coordinator. Each Contributor is separately responsible for conducting and complying with the DPIA obligations if so required by their local authorities.
14. Further agreements regarding privacy responsibilities.	If the arrangements in this matrix appear to be incomplete or incorrect, the parties shall amend this matrix so as to be compliant with the GDPR.

APPENDIX D: MODEL ACCESSION FORM

Accession of a Party to the EuRREB Registries

[**NAME INSTITUTE**], having its registered office and principal place of business at [**ADDRESS INSTITUTE**], lawfully represented by [NAME of the institute's authorized signatory], in her/his function as [**FUNCTION of the institute's authorized signatory**], hereinafter referred to as "[**SHORT NAME INSTITUTE**]";

Hereby consents to become a Contributor to the EuRREB Registries identified above and accepts all the rights and obligations of a Contributor starting [DATE receiving registries account].

Academisch Ziekenhuis Leiden, also acting under the name Leiden University Medical Center, having its registered office and principal place of business in at Albinusdreef 2 Leiden, the Netherlands, legally represented by mr. H.B.M. Onstein of the Coordinator's authorized signatory, Managing Director, hereinafter referred to as "**COORDINATOR"**

Acting on behalf of the Project Management Team and Steering Committee in accordance with Section 5 of the Registries Joint Data Registry Agreement hereby certifies that the Steering Committee has accepted the accession of [**SHORT NAME INSTITUTE**] to the EuRREB Registries.

Each Party agrees that this declaration of accession will be executed in electronic PDF format only and the Contributor signing this declaration of accession explicitly acknowledges and agrees that its signature in such format shall be regarded as an original signature and that this declaration of accession shall be effective upon delivery by electronic mail to the Coordinator and thereafter shall be deemed an original signed agreement.

[insert name of your institute]

Signature:

Name:
Title:
Date: Place:

Leiden University Medical Center (LUMC)
Acting as Coordinator of the EuRREB Registries in accordance with the Joint Data Registry Agreement

Signature:

Name: H.B.M. Onstein
Title: Managing Director
Date: Place: Leiden, The Netherlands

APPENDIX E: MAIL OF APPROVAL FORMAT

Dear Researcher,

The Data Access Committee of the EuRREB Registries has received in good order the study proposal [**NAME PROJECT]** you submitted to it. The proposal was subsequently judged dated [**DATE]**.

The Data Access Committee considered the following documents in its review:

- Data Request Form version [**number**], dated [**DATE**].

The Data Access Committee of the EuRREB Registries has determined that the study falls within the Main Objectives as stated in the EuRREB Registries Joint Data Registry Agreement' which justifies the release of data for the execution of the aforementioned Study proposal.

Pricing category
Please note that access to EuRREB data is subject to the applicable conditions as defined in the EuRREB Pricelist (attached to this message). Based on the status of the applicant, one of the following categories applies:

- Pharma company (Funding)
- ERN network member (discount rate)
- No-Contributor (No-Funding)

The applicable category and any associated financial conditions will be confirmed separately, if relevant, prior to data release.

Please note: The Data will not be made available until you have sent a confirmation email accepting the terms of use.

The Data Access Committee reminds you of your duties with respect to the Data. You are expected to:

(a) use the Data in accordance with the GDPR and other applicable laws and regulations. You are fully responsible for this.

b) to make no attempt to trace the identity of the patients.

(c) Use the Data only for the approved Study Proposal. In the event of deviations or changes to the study proposal, the Data Access Committee has the right, in its sole discretion, to terminate access to the Database without liability.

(d) not disclose or provide access to the Data to any third party without the prior written consent of the Data Access Committee. In the event that you send data to a third party for the purposes of an approved study proposal, you must enter into a contract with that party.

(e) report twice a year the progress and results of the study to the Coordinator.

(f) publish scientifically in accordance with the provisions of the EuRREB Registry Joint Data Registry Agreement and publication guidelines (attached to this message).

(g) immediately report any data breach if it still occurs despite all the necessary safeguards. A data breach is any security incident involving data received from EuRREB that results in the accidental or unlawful loss, destruction, alteration, unauthorised access to, disclosure of, or misuse of such data by a researcher, whether intentional or unintentional. On behalf of the Data Access Committee of the EuRREB Registries, I wish you luck with your research project.

Sincerely,

Name, project Manager EuRREB Registries on behalf of the Project Management Team and

[NAME], Chairman of the EuRREB Registries Data Access Committee

APPENDIX F: FINANCIAL ARRANGEMENTS

If applicable, please specify any agreed financial arrangements.

APPENDIX G: DECLARATION OF ACCEPTANCE (Coordinator)

Declaration of acceptance by the Coordinating Partner of the Joint Data Registry Agreement of the "EuRREB Registries"

Academisch Ziekenhuis Leiden, also acting under the name Leiden University Medical Center, having its registered office and principal place of business at Albinusdreef 2 Leiden, the Netherlands legally represented by **mr. H.B.M. Onstein, Managing director, hereinafter referred to as "Coordinator"**

hereby accepts all the rights and obligations stated in the aforementioned Agreement effective **10th of March 2026**.

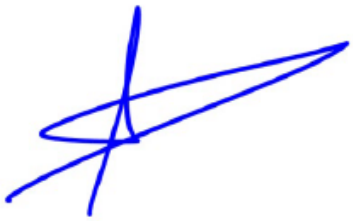
This Declaration of Acceptance has been executed in 2 originals, duly signed by the undersigned authorized representative.

Leiden University Medical Center
Signature(s)



Name(s) legal representative H.B.M. Onstein
Title(s) Managing director

12 March 2026, Leiden, the Netherlands



Registries coordinator N.M. Appelman-Dijkstra
Title(s) Professor, MD, PhD

12 March 2026, Leiden, the Netherlands

This Appendix H applies only to Contributors established outside the EEA in the absence of an Adequacy Decision, in case they receive data from the Registries for the purpose of a Study

APPENDIX H: STANDARD CONTRACTUAL CLAUSES

EU STANDARD CONTRACTUAL CLAUSES vs. 4 June 2021 (MODULE ONE: Transfer controller to controller)

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

(iii) Clause 9 – N.A.;

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

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 –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) 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) (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

N.A.

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. (10) 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 body (11) 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 hird-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) [Where the data exporter is established in an EU Member State:] 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.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, 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 ([12]);

(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). [For Module Three: The data exporter shall forward the notification to the controller.]

(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 [for Module Three:, if appropriate in consultation with the controller]. 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 [for Module Three: the controller or] 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

OPTION 1: 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.

---

(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, 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.

(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.

(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.

(4) 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.

(5) See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

(6) 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 purposes of these Clauses.

(7) This includes whether the transfer and further processing 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.

(8) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(9) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(10) 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.

(11) The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(12) 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.

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.

ANNEX I

A. LIST OF PARTIES

See Appendix A "EuRREB Registries" Joint Data Registry Agreement

B. DESCRIPTION OF TRANSFER

See Appendix C "EuRREB Registries" Joint Data Registry Agreement

C. COMPETENT SUPERVISORY AUTHORITY

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

Autoriteit Persoonsgegevens (Dutch Data Protection Authority), Bezuidenhoutseweg 30, 2594 AV The Hague, The Netherlands

ANNEX II

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

MODULE ONE: Transfer controller to controller

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.

Situation: Data exporter provides Pseudonymised data. The data exporter has the confidentiality of the Pseudonymised data classified as medium. Availability is classified as low.

Data are Pseudonymised by the data exporter. Keys are only available for the data exporter.

Transport

- Data are transported by secure, encrypted means., Encryption meeting NIST standards
- Data importer will verify and confirm receipt of data.

Access and storageTechnical measures.
The technical measures include:

- Physical measures for access security, including organizational control.
- Access only allowed for qualified persons and necessity to access the data.
- Access accounts are personal. Shared accounts for accessing the data are not available.
- Access to the data is logged.
- Multi factor authentication is required when accessing data outside the buildings controlled by the data importer.
- Measures against malicious software (anti-virus, anti-spam, etc) on endpoints and servers;
- Outer perimeter security through state-of-the art Firewalls;
- Securing network connections via SSL (Secure Socket Layer);
- Encryption of personal data during transmission;
- Encryption of Pseudonymised data in rest;
- Encryption methods and implementation will meet current National Institute of Standards and Technology (NIST) advises
- Monitoring of network traffic on suspicious behavior.

Organizational measures
The organizational measures include:

- A written established security policy including implementation based on a periodic risk assessment;
- Security policy is periodically reviewed and adapted;
- Data importer continuously monitors incidents, performance of the IT systems and continuously improves security.
- Responsibilities for information security have been assigned;
- Employee confidentiality obligations;
- Screening of new employees;
- Change Management procedures for changes in data or in information processing;

- Patch management ensures that patches are timely applied;
- Powers are granted based on the "Need-to-know" principle;
- Periodic internal audits to ensure compliance with standards and requirements
- Periodic external audits to ensure compliance with standards and requirements
- Mandatory awareness training for employees with regard to security and privacy;
- User and administrator activities are logged. Logging is periodically checked;
- Data importer will treat passwords confidentially and adequately secure them. Only personal accounts will be used no shared accounts. In the event of loss or (suspected) misuse of the login codes and passwords, Data importer will immediately take all measures to limit the damage that may ensue.
- Password requirements will meet the current National Institute of Standards and Technology (NIST) advises
- The need for access to the data is periodically checked. When access is not needed (any more) access privileges are revoked a.s.a.p
- Responsibilities for the data are assigned to one or two individuals
- Data importer can demonstrate effectiveness of measures taken..

Other measures:

- Data importer shall not attempt in any way to identify or contact the individuals from whom such Data were collected, Data importer shall not link the Data to other data
- After termination of this agreement data including back-up will be secure erased. Erasure will meet the current NIST Guideline Guidelines for Media Sanitization Data importer will confirm erasure and way of erasure.
- Interdiction of Publication of identifiable data.
- DPA with processors,

Secure data processing can be demonstrated by certification e.g. for ISO 27001 and 27002, third party memorandum, binding corporate rules etc. The data importer has the following certification(s) or assurance(s) of secure data processing:

ANNEX III

LIST OF SUB-PROCESSORS

N.A.