

## **Joint Controller Agreement regarding the processing and sharing of personal data in accordance with Article 26 (1) GDPR**

### **Between:**

1. DEUTSCHES ZENTRUM FÜR LUFT - UND RAUMFAHRT EV – DLR established in LINDER HOHE, 51147, KOLN, DE, the Coordinator of the consortium, and
2. AGENCE NATIONALE DE LA RECHERCHE – ANR, established in 86 RUE REGNAULT, 75013, PARIS, FR
3. VLAAMSE GEWEST - VL O, established in AVENUE DU PORT 88, 1000, BRUSSEL, BE
4. INSTITUTO ARAGONES DE CIENCIAS DE LA SALUD – IACS, established in AVENIDA SAN JUAN BOSCO 13, 50009, ZARAGOZA, ES
5. FONDAZIONE TOSCANA LIFE SCIENCES – TLS, established in VIA FIORENTINA 1, 53100, SIENA, IT
6. NORGES FORSKNINGSRAD - THE RESEARCH COUNCIL OF NORWAY, established in DRAMMENSVEIEN 288, 0283, OSLO, NO
7. MINISTERO DELLA SALUTE – IT MoH, established in Via Giorgio Ribotta 5, 00144, ROMA, IT
8. INSTITUTO DE SALUD CARLOS III – ISCIII, established in MONFORTE DE LEMOS 5, 28029, MADRID, ES
9. SCIENCE FOUNDATION IRELAND – SFI, established in THREE PARK PLACE, HATCH STREET UPPER, D002FX65, DUBLIN, IE
10. SÄCHSISCHES STAATSMINISTERIUM FÜR WISSENSCHAFT, KULTUR UND TOURISMUS – SMWK, established in WIGANDSTRASSE 17, 01097, Dresden, DE
11. FONDAZIONE TELETHON ETS - FONDAZIONE TELETHON ETS, established in VIA VARESE 16/B, 00185, ROMA, IT
12. FONDAZIONE REGIONALE PER LA RICERCA BIOMEDICA – FRRB, established in PIAZZA CITTA DI LOMBARDIA 1, 20124, MILANO, IT
13. FONDS ZUR FÖRDERUNG DER WISSENSCHAFTLICHEN FORSCHUNG – FWF, established in GEORG-COCH-PLATZ 2, 1010, WIEN, AT
14. THE HEALTH RESEARCH BOARD – HRB, established in 67 72 LOWER MOUNT STREET, D02 H638, DUBLIN, IE
15. LIETUVOS MOKSLO TARYBA – LMT, established in Gedimino 3, LT-01103, Vilnius, LT
16. MINISTRY OF HEALTH - CSO-MOH, established in YIRMIYAHU 39, 9101002, JERUSALEM, IL
17. SIHTASUTUS EESTI TEADUSAGENTUUR – ETAg, established in SOOLA 8, 51004, TARTU, EE
18. TÜRKİYE BİLİMSEL VE TEKNOLOJİK ARASTIRMA KURUMU – TÜBİTAK, established in Atatürk Bulvarı 221, 06100, ANKARA, TR
19. EIT HEALTH EV, established in MIES-VAN-DER-ROHE-STRASSE 1 C, 80807, MUNCHEN, DE
20. VERKET FÖR INNOVATIONSSYSTEM - VINNOVA SWEDISH AGENCY FOR INNOVATION SYSTEMS – VINNOVA, established in MASTER SAMUELSG 56, 10158, STOCKHOLM, SE
21. NARODOWE CENTRUM BADAN I ROZWOJU – NCBR, established in UL. CHMIELNA 69, 00-801, WARSZAWA, PL

22. AGENCIA DE INVESTIGACAO CLINICA E INOVACAO BIOMEDICA – AICIB, established in RUA DE SANTA CATARINA 1288, 4000-447, PORTO, PT
23. FUNDACAO PARA A CIENCIA E A TECNOLOGIA – FCT, established in AVENIDA D CARLOS I 126, 1249 074, LISBOA, PT
24. ZORGONDERZOEK NEDERLAND ZON – ZON, established in Laan Van Nieuw Oost Indie 334, 2593 CE, DEN HAAG, NL
25. FONDS NATIONAL DE LA RECHERCHE – FNR, established in 2 AVENUE DE L'UNIVERSITE, 4365, ESCH-SUR-ALZETTE, LU
26. REGIONE TOSCANA – RT, established in Palazzo Strozzi Sacratì - Piazza del Duomo 10, 50122, FIRENZE, IT
27. SERVICE PUBLIC DE WALLONIE – SPW, established in Place de la Wallonie 1, 5100, Namur, BE
28. FONDS DE LA RECHERCHE SCIENTIFIQUE- FNRS, established in RUE D'EGMONT 5, 1000, BRUXELLES, BE
29. DEPARTAMENT DE SALUT - GENERALITAT DE CATALUNYA – DS CAT, established in Trav. de les Corts (Pavelló Ave Maria) 131-159, 08028, BARCELONA, ES
30. COMUNIDAD FORAL DE NAVARRA - GOBIERNO DE NAVARRA - COMUNIDAD FORAL DE NAVARRA – CFN, established in AVENIDA CARLOS III 2, 31002, PAMPLONA, ES
31. SOTSIAALMINISTEERIUM – MSAE, established in Suur-Ameerika 1, 10122, TALLINN, EE
32. FONDS VOOR WETENSCHAPPELIJK ONDERZOEK-VLAANDEREN - FWO, established in LEUVENSEWEG 38, 1000, BRUSSEL, BE
33. INNOVAATIO RAHOITUSKESKUS BUSINESS FINLAND – BFRK, established in PO BOX 69, 00101, HELSINKI, FI
34. VETENSKAPSRÅDET - SWEDISH RESEARCH COUNCIL – SRC, established in BOX 1035, 101 38, STOCKHOLM, SE
35. SUOMEN AKATEMIA – AKA, established in HAKANIEMENRANTA 6, 00531, HELSINKI, FI
36. BIOBANKS AND BIOMOLECULAR RESOURCES RESEARCH INFRASTRUCTURE CONSORTIUM (BBMRI-ERIC) - BBMRI-ERIC, established in NEUE STIFTINGTALSTRASSE 2/B/6, 8010, GRAZ, AT
37. INNOVATIONSFONDEN - DANMARK INNOVATIONSFOND DANISH INNOVATION FOUNDATION – IFD, established in ØSTERGADE 26 A, 1100, KØBENHAVN K, DK
38. NEMZETI KUTATASI FEJLESZTESI ES INNOVACIOS HIVATAL – NKFIH, established in KETHLY ANNA TER 1, 1077, BUDAPEST, HU
39. LATVIJAS ZINATNES PADOME – LZP, established in SMILSU IELA 8, 1050, RIGA, LV
40. VICE-PRESIDENCIA DO GOVERNO REGIONAL DOS AÇORES – VP GRA, established in LARGO PRIOR DO CRATO, 9700-157, ANGRA DO HEROÍSMO, PT
41. COMISSAO DE COORDENACAO E DESENVOLVIMENTO REGIONAL DO CENTRO – CCDRC, established in RUA BERNARDIM RIBEIRO 80, 3000-069, COIMBRA, PT
42. RANNSOKNAMIDSTOD ISLANDS – Rannis, established in BORGARTUNI 30, 105, REYKJAVIK, IS
43. Ministero dell'università e della ricerca – MUR, established in Via Michele Carcani 61, 00153, Roma, IT
44. DEPARTAMENTO DE SALUD GOBIERNO VASCO – DPTO SALUD, established in Donostia-San Sebastián, 1, 01010, VITORIA-GASTEIZ, ES
45. UNITATEA EXECUTIVA PENTRU FINANTAREA INVATAMANTULUI SUPERIOR A CERCETARII DEZVOLTARII SI INOVARII – UEFISCDI, established in STR D I MENDELEEV 21-25, 010362, BUCURESTI, RO

46. BUNDESMINISTERIUM FUER GESUNDHEIT – BMG, established in ROCHUSTRASSE 1, 53123, BONN, DE
47. BUNDESMINISTERIUM FUER BILDUNG UND FORSCHUNG – BMBF, established in Heinemannstrasse 2, 53175, BONN, DE
48. BUNDESMINISTERIUM FUER BILDUNG, WISSENSCHAFT UND FORSCHUNG – BMBWF, established in MINORITENPLATZ 5, 1010, VIENNA, AT
49. FONDS INNOVEREN EN ONDERNEMEN – HERMESFOND – FIO, established in BOULEVARD DU ROI ALBERT II 35, 1030, BRUXELLES, BE
50. SWISS INNOVATION AGENCY – INNOSUISSE, established in EINSTEINSTRASSE 2, 3003 BERN, CH

hereinafter, jointly or individually, referred to as “Joint Controllers” or “Parties” relating to the project entitled European Partnership for Personalised Medicine, in short: EP PerMed.

## Preamble

The German Aerospace Center (DLR) is the national center of aerospace research of the Federal Republic of Germany. Its research and development activities in aeronautics, aerospace, energy, transport, digitisation and security are incorporated into national and international cooperative ventures. DLR coordinates the European Partnership for Personalised Medicine, in short EP PerMed. This agreement lays down the rules for the data management which will be obtained by implementation of the Joint Transnational Calls (JTCs) and activities of the EP PerMed under the European Commission Grant Agreement No. 101137129 (Grant Agreement), and is made on 1st November 2023, hereinafter referred to as the ‘Effective Date’.

## Section 1 - Definitions

(1) In this Agreement, the legal definitions and terms of Articles 4 and 5 of the General Data Protection Regulation (EU) 2016/679 (hereinafter: "GDPR") shall apply.

(2) According to Article 4 (1) GDPR ‘personal data’ means any information relating to an identified or identifiable natural person (‘data 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.

(3) According to Article 4 (2) GDPR ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(4) According to Article 4 (7) GDPR ‘controller’ (or Joint Controller) means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

(5) Special categories of (sensitive and/or restricted) personal data are personal data in accordance with Article 9 GDPR, from which the racial and ethnic origin, political opinions,

religious or ideological beliefs or trade union membership of those affected can be deduced, personal data in accordance with Art. 10 GDPR on criminal convictions and offences or related security measures as well as genetic data pursuant to Article 4 (13) GDPR, biometric data pursuant to Article 4 (14) GDPR, health data pursuant to Article 4 (15) GDPR and data on the sexual life or sexual orientation of a natural person.

(6) According to Article 4 (21) GDPR 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51 GDPR.

(7) According to Article 4 (23) GDPR cross-border processing' means either:

(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

## **Section 2 - Subject of the Agreement**

(1) This agreement regulates the rights and obligations of the parties in the joint processing of personal data. This agreement applies to all activities in which employees of the parties or processors commissioned by them process personal data for the controllers. The parties have jointly determined the means and purposes of the processing activities described in more detail below.

(2) The term of this agreement is based on the term of the Consortium Agreement, unless the following provisions result in further obligations or rights of termination.

(3) Personal data are processed in the European Partnership EP PerMed. Depending on the process stage, the processing of these data takes place on secure servers or IT-infrastructures as described in Annex 1. The parties shall define the process stages in which personal data are processed under joint responsibility (Article 26 GDPR).

(4) The provision of the contractually agreed data processing activities shall take place exclusively in a member state of the European Union or another contracting state of the Agreement on the European Contractual Area/European Economic Area. Any relocation of partial services or the entire service to a third country requires prior notification to the other party or parties in writing or in documented electronic format and may only take place if the special requirements of Articles 44 to 49 GDPR shall be fulfilled.

## **Section 3 - Responsibilities of the parties**

(1) Within the scope of joint responsibility, the parties are responsible for the processing of personal data as described in the GDPR, this agreement, and Annex 1. The subject of the processing, the legal basis of which is the GDPR, are the following types/categories of data:

- General data/Private contact details (names, nationality, professional affiliation/contact data (addresses, telephone numbers and e-mail-addresses), gender, bank data (if applicable for reimbursement)
- Service and IT (use) data (access data, image/video data)
- Professional data (qualifications, curriculum vitae, content of unpublished scientific proposals)

There will be not carried out any processing of the special categories of data (Article 9 of GDPR). Such types of data will not be collected or shared between the Joint Controllers of Personal Data in the framework of this cooperation.

Other specific data that can be sensitive but that are not included under the special categories of data (e.g. bank data) that may need to be shared between the parties shall only be shared by secure e-mail between authorised persons who need those data for the performance of their functions.

Personal data is only kept for the time required for the operations for which it was collected and in compliance with the regulations on the protection of personal data in force.

Each of the Parties ensures that the data retention periods are respected.

#### **Section 4 - Responsibilities and obligations of the parties**

(1) The parties have jointly determined the main purposes of the processing which are described in Annex 1.

(2) The means of the processing are jointly determined by the parties, either the material means, the software or even the human resources affected to the processing.

(3) Each party shall ensure compliance with the legal provisions, in particular the lawfulness of the data processing carried out by it, also within the scope of joint responsibility. The parties shall take all necessary technical and organisational measures to ensure that the rights of the data subjects, in particular in accordance with Articles 12 to 23 GDPR, can be or are guaranteed at all times within the statutory time limits.

(4) The parties ensure that only personal data are collected which are absolutely necessary for the lawful processing and for which the purposes and means of processing are laid down by Union law or Member State law. Furthermore, all contracting parties shall observe the principle of data minimization within the meaning of Article 5 (1) (c) GDPR.

(5) The parties shall store the personal data in a structured commonly used and machine-readable format.

(6) Documentation within the meaning of Article 5 (2) of the GDPR, which serves as proof of proper data processing, shall be retained by each party beyond the end of the contract in accordance with the legal powers and obligations.

#### **Section 5 - Provision of information on data processing**

(1) The parties undertake to provide the data subject free of charge with the information required under Articles 13 and 14 GDPR in a precise, transparent, intelligible and easily accessible form in plain and simple language.

(2) The parties agree that each party appointed in Annex 1 to be the responsible data processor shall provide the information for the processing of personal data in their responsible scope described in Annex 1 in accordance to sections 3 and 4 of this agreement.

#### **Section 6 - Requests and data subject rights**

(1) Insofar as a data subject approaches one of the parties in the exercise of his or her data subject rights, in particular for information or correction and deletion of his or her personal data, the parties undertake to forward this request to the appropriate party or parties without delay, irrespective of the obligation to guarantee the data subject right. The latter shall be obliged to

provide the requesting party with the information from its/their sphere of activity necessary for the provision of information without delay.

(2) The parties shall provide each other with the necessary information from their respective spheres of activity as required. The contact persons of the parties responsible for this are listed in Annex 3. The other party or parties shall be informed immediately of any change of the respective contact person (e.g. via e-mail).

(3) Data subjects can assert their rights under Articles 15 to 22 GDPR against all contracting parties. They will receive the information from the contracting party with whom the request was made.

(4) The parties undertake to provide the data subjects with the information to which they are entitled pursuant to Art. 15 GDPR upon request. If the data subject makes the request electronically, the information shall be provided by the party with whom the request was made in a commonly used electronic format within one month, unless the data subject indicates otherwise.

(5) If personal data is to be deleted, the parties shall inform each other beforehand. The other party or parties may object to the deletion for a justified reason, for example if it has/they have a legal obligation to retain the data.

(6) The parties undertake to make the essential content of the data protection joint responsibility agreement available to the data subjects (Article 26 (2) GDPR).

## **Section 7 - Notification obligations**

The parties shall inform each other immediately and in full if they discover errors or irregularities with regard to data protection provisions during an audit of the processing activities.

## **Section 8 – Data breaches**

The parties shall be subject to the notification and notification/communication obligations resulting from Art. 33, 34 GDPR vis-à-vis the supervisory authority and the persons affected by a personal data breach for their respective sphere of activity. The parties shall inform each other without undue delay of the notification of personal data breaches to the supervisory authority and shall each forward to the others without undue delay the information necessary to implement the notification.

If one of the partners suffers an incident suggesting a breach of personal data subject to joint processing, it shall immediately inform the other partners of this incident and without delay after its discovery. This information must :

- describe the likely origin of the personal data breach and the nature of the breach including, if possible, the categories and approximate number of persons affected by the breach and the categories and approximate number of personal data records affected;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by [to be completed] to remedy the personal data breach, including, where appropriate, measures to mitigate any negative consequences.
- exchanging all relevant information in order to qualify the incident, determine whether a personal data breach has occurred and remedy the difficulties encountered;
- minimise the prejudice suffered by each of the Parties and the persons concerned;

Each Party shall keep an incident log indicating the facts concerning the personal data breach suffered, its effects and the measures taken to remedy it

## **Section 9 - Supervisory Authority procedure**

The parties and, where applicable, their representatives shall cooperate with the supervisory authority in the fulfilment of their obligations upon request.

## **Section 10 - Security of processing**

(1) The parties shall ensure within their sphere of activity that all employees involved in data processing maintain the confidentiality of the data in accordance with Articles 28 (3), 29 and 32 of the GDPR for the duration of their employment as well as after termination of the employment relationship and that they are appropriately obligated to maintain data secrecy and instructed in the data protection provisions relevant to them before taking up their employment.

(2) The parties shall independently ensure that they comply with all statutory retention obligations existing in relation to the data. To this end, they shall take appropriate data security precautions (Art. 32 et seq. GDPR). This applies in particular in the event of termination of the cooperation.

(3) The implementation, pre-setting and operation of the systems shall be carried out in compliance with the requirements of the GDPR and other sets of regulations, in particular in compliance with the principles of data protection by design and data protection-friendly default settings, as well as using appropriate state-of-the-art technical and organisational measures.

(4) To this end, and taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the parties shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

(5) The personal data to be processed in the course of handling the services on the data processing tools listed in Annex 1 shall be stored on specially protected servers.

## **Section 11 - Appointment of processors**

(1) In order to comply with the rights and obligations within the scope of this Agreement (see Section 3 of this Agreement), the parties are authorised to commission processors used as subcontractors. The chosen processor shall provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subjects.

(2) Each party undertakes to conclude a contract in accordance with Article 28 GDPR when appointing processors and to inform the other party of the appointment prior to the conclusion of the processing agreement. Each party shall have the right to prohibit the commissioning of a specific processor if there are important reasons for doing so.

(3) The parties shall inform each other in good time of any intended change with regard to the use or replacement of processors used as subcontractors and shall only engage such subcontractors who meet the requirements of data protection law (according to GDPR) and the stipulations of this Agreement.

(4) For the purposes of this provision, subcontracted services do not include services that the parties use from third parties as an ancillary service to support the performance of the contract, such as telecommunications services and maintenance. However, the parties are obliged to conclude appropriate and legally compliant contractual agreements and to take control measures in order to ensure the protection and security of personal data, even in the case of subcontracted services. Third parties are parties that are not EP PerMed beneficiaries, associated partners or affiliated entities.

## **Section 12 - Record of processing activities and data protection impact assessment**

(1) The parties shall include the processing activities in the processing directory in accordance to Article 30 (1) GDPR, including and in particular with a note on the nature of the processing operation under joint or sole responsibility.

(2) Where a data protection impact assessment is required in accordance with Article 35 GDPR, the parties shall support each other.

## **Section 13 - Liability**

(1) The parties shall be liable to data subjects in accordance with the regulations set out in Article 82 GDPR.

(2) The parties shall each indemnify themselves against liability insofar as a party is able to prove that it is not responsible in any respect for the circumstance which caused the damage to a data subject. In all other respects, Article 82 (5) GDPR shall apply.

(3) Notwithstanding the provisions of this contract, the parties shall be jointly liable towards the data subjects as to external relations for the damage caused by processing which does not comply with the GDPR.

(4) The parties shall be liable internally, without affecting the provisions of this contract, for any damage caused within their respective spheres of activity solely.

## **Section 14 – Transfer of personal data**

In the event of data transfer outside the European Union, the parties undertake to ensure that the destination country has appropriate safeguards within the meaning of the GDPR. Failing this, the parties undertake to sign the standard contractual clauses set out in Annex 4.

## **Section 15 - Severability, final provisions**

(1) Amendments and supplements to this agreement must be made in writing or in a documented electronic format. This also applies to a waiver regarding this formal requirement.

(2) Should any provision of this agreement be or become invalid or void, either in whole or partially, or due to a change to the legal framework or as a result of supreme court rulings or in any other way, or should this agreement contain any gaps, the parties agree that the remaining provisions of this agreement shall remain unaffected and valid. In this case, the parties undertake, taking into account the principle of equity and good faith, to agree on a valid provision in place of the invalid provision which comes as close as possible to the meaning and purpose of the invalid provision and which the parties would have agreed on at the time



of conclusion of the contract if they had known or foreseen the invalidity or ineffectiveness. The same shall apply if this agreement should contain a loophole.

(3) This agreement is governed by the General Data Protection Regulation and German substantive law.

(4) This agreement is drafted in English.

### **Annexes**

Annex 1 - Responsibilities of the parties

Annex 2 - Subcontractor

Annex 3 - List of contact persons

Annex 4 - Appropriate safeguards for third country transfers in accordance with Articles 44 to 49 GDPR

### **Date and signatures**

.....  
(location, date signed)

.....  
(DLR)

**75012 Paris,**

.....  
(location, date signed)

.....  
**(party 2)**

P2 ANR  
Agence Nationale de la Recherche  
50 Avenue Daumesnil  
75012 Paris  
France

## Date and signatures

**1000 Bruxelles,**

.....

.....  
(location, date signed)

.....

.....  
(party 3)

P03 VLO-EWI  
VLAAMSE GVLAAMSE  
GEWESTEWEST  
Avenue du Port 88 000I  
1000 Bruxelles  
Belgium

## Date and signatures

50009 Zaragoza,

.....

.....  
(location, date signed)

.....

.....  
(party 4)

P04 IACS  
INSTITUTO ARAGONES DE CIENCIAS  
DE LA SALUD - Health Sciences  
Institute in Aragon (IACS)  
Avenida San Juan Bosco 13  
50009 Zaragoza  
Spain

## Date and signatures

**53100 Siena,**

.....

.....  
(location, date signed)

.....

.....  
(party 5)

P05 TLS  
Fondazione Toscana Life Sciences  
Via Fiorentina 1  
53100 Siena  
Italy

## Date and signatures

0283 Oslo,

.....

.....  
(location, date signed)

.....

.....  
(party 6)

P06 RCN  
The Research Council of Norway  
DRAMMENSVEIEN 288 000  
0283 Oslo  
Norway

## Date and signatures

.....

**00144 Roma,**

.....  
(location, date signed)

.....

.....  
(party 7)

P07 IT-MoH  
MINISTERO DELLA SALUTE  
Via Giorgio Ribotta 5  
00144 Roma  
Italy

## Date and signatures

**28029 Madrid,**

.....

.....  
(location, date signed)

.....

.....  
(party 8)

P08 ISCIII  
Instituto de Salud Carlos III  
MONFORTE DE LEMOS 5 000  
28029 Madrid  
Spain

## Date and signatures

.....

.....

**D002FX65 Dublin,**

.....  
(location, date signed)

.....  
(party 9)

P09 SFI  
Science Foundation Ireland  
THREE PARK PLACE, HATCH STREET  
UPPER 000  
D002FX65 Dublin  
Ireland



## Date and signatures

**01097 Dresden,**

.....

.....  
(location, date signed)

.....

.....  
(party 10)

P10 SMWK  
Saxon State Ministry for Science, Culture  
and Tourism  
Wigardstr. 17  
01097 Dresden  
Germany

## Date and signatures

**00185 Roma,**

.....

.....  
(location, date signed)

.....

.....  
(party 11)

P11 FTELE  
Fondazione Telethon ETS  
Via Varese 16/b 000  
00185 Roma  
Italy

## Date and signatures

**20124 Milano,**

.....

.....  
(location, date signed)

.....

.....  
(party 12)

P12 FRRB  
Fondazione Regionale per la Ricerca  
Biomedica  
Piazza Citta di Lombardia 1  
20124 Milano  
Italy

## Date and signatures

**1010 Wien,**

.....  
(location, date signed)

.....  
(party 13)

P13 FWF  
Fonds zur Förderung der  
wissenschaftlichen Forschung  
Georg-Coch-Platz 2  
1010 Wien  
Austria

## Date and signatures

.....

.....

**D02 H638 Dublin,**

.....  
(location, date signed)

.....  
(party 14)

P14 HRB  
Health Research Board  
67 72 LOWER MOUNT STREET  
D02 H638 Dublin  
Ireland

## Date and signatures

**LT-01103 Vilnius,**

.....

.....  
(location, date signed)

.....

.....  
(party 15)

P15 LMT  
Lietuvos mokslo taryba (Research  
Council of Lithuania)  
Gedimino 3  
LT-01103 Vilniusn  
Lithuania

## Date and signatures

9103002 Jerusalem,

.....

.....  
(location, date signed)

.....

.....  
(party 16)

P16 CSO-MoH  
Medical Research & Development Fund  
for Health Services  
P.O.B 3117  
9103002 Jerusalem  
Israel

## Date and signatures

**51004 Tartu,**

.....

.....  
(location, date signed)

.....

.....  
(party 17)

P17 ETAG  
SIHTASUTUS EESTI  
TEADUSAGENTUUR  
Soola 8  
51004 Tartu  
Estonia



## Date and signatures

06100 Ankara,

.....

.....  
(location, date signed)

.....

.....  
(party 18)

P18 TUBITAK  
The Scientific and Technological  
Research Council of Turkey  
Ataturk Bulvari 221  
06100 Ankara  
Türkiye

## Date and signatures

80807 München,

.....  
(location, date signed)

.....  
(party 19)

P19 EITH  
EIT Health eV  
Mies-van-der-Rohe-Strasse 1 C  
80807 München  
Germany

.....  
(party 19.1)

P19.1 EIT BENE  
EIT Health BENE

.....  
(party 19.2)

P19.2 EITH SCAN  
EIT Health Scan

## Date and signatures

**10158 Stockholm,**

.....

.....  
(location, date signed)

.....

.....  
(party 20)

P20 VINNOVA  
VINNOVA Sweden's Innovation Agency  
MASTER SAMUELSG 56  
10158 Stockholm  
Sweden

## Date and signatures

00-801 Warszawa,

.....

.....  
(location, date signed)

.....

.....  
(party 21)

P21 NCBR  
National Centre for Research and  
Development  
Ul. Chmielna 69  
00-801 Warszawa  
Poland

## Date and signatures

**4000-447 Porto,**

.....

.....  
(location, date signed)

.....

.....  
(party 22)

P22 AICIB  
Agency for Clinical Research and  
Biomedical Innovation  
RUA DE SANTA CATARINA 1288 000  
4000-447 Porto  
Portugal

## Date and signatures

1249 074 Lisboa,

.....

.....  
(location, date signed)

.....

.....  
(party 23)

P23 FCT  
Fundação para a Ciência e a Tecnologia  
AVENIDA D CARLOS I 126 000  
1249 074 Lisboa  
Portugal

## Date and signatures

.....

.....

**2593 CE Den Haag,**

.....

(location, date signed)

.....  
(party 24)

P24 ZonMw  
Zorgonderzoek Nederland ZON  
Laan Van Nieuw Oost Indie 334 93245  
2593 CE Den Haag  
Netherlands

## Date and signatures

.....

.....

**L-4365 Esch-Sur-Alzette,**

.....  
(location, date signed)

.....  
(party 25)

P25 FNR  
Fonds National de la Recherche  
2 Avenue de l'Universite  
L-4365 Esch-Sur-Alzette  
Luxembourg



## Date and signatures

**50122 Firenze,**

.....

.....  
(location, date signed)

.....

.....  
(party 26)

P26 RT  
Regione Toscana – Tuscany Region  
Palazzo Strozzi Sacratì - Piazza del  
Duomo 10  
50122 Firenze  
Italy

## Date and signatures

5100 Namur,

.....

.....  
(location, date signed)

.....

.....  
(party 27)

P27 SPW EER  
SERVICE PUBLIC DE WALLONIE  
Place de la Wallonie 1  
5100 Namur  
Belgium

## Date and signatures

**1000 Bruxelles,**

.....

.....  
(location, date signed)

.....

.....  
(party 28)

P28 FRS-FNRS  
FONDS DE LA RECHERCHE  
SCIENTIFIQUE- FNRS  
RUE D'EGMONT 5 000  
1000 Bruxelles  
Belgium

## Date and signatures

08028 Barcelona,

.....

.....  
(location, date signed)

.....

.....  
(party 29)

P29 DS-CAT  
DEPARTAMENT DE SALUT -  
GENERALITAT DE CATALUNYA  
Trav. de les Corts (Pavelló Ave Maria)  
131-159  
08028 Barcelona  
Spain

## Date and signatures

**31002 Pamplona,**

.....

.....  
(location, date signed)

.....

.....  
(party 30)

P30 CFN // GN  
Comunidad Foral de Navarra  
AVENIDA CARLOS III 2  
31002 Pamplona  
Spain

## Date and signatures

**10122 Tallin,**

.....

.....  
(location, date signed)

.....

.....  
(party 31)

P31 MoSAE  
Ministry of Finance  
Suur-Ameerika 1  
10122 Tallin  
Estonia

## Date and signatures

**1000 Bruxelles,**

.....

.....  
(location, date signed)

.....

.....  
(party 32)

P32 FWO  
FONDS VOOR WETENSCHAPPELIJK  
ONDERZOEK-VLAANDEREN - FONDS  
WETENSCHAPPELIJK ONDERZOEK  
LEUVENSEWEG 38 000  
1000 Bruxelles  
Belgium

## Date and signatures

00101 Helsinki,

.....  
(location, date signed)

.....  
(party 33)

P33 BFRK  
Innovaatorahoituskeskus Business  
Finland  
PO BOX 69 000  
00101 Helsinki  
Finland

.....  
(party 33.1)

P33.1 BFOY  
Business Finland Oy



## Date and signatures

**10138 Stockholm,**

.....

.....  
(location, date signed)

.....

.....  
(party 34)

P34 SRC  
Swedish Research Council  
BOX 1035 1035  
10138 Stockholm  
Sweden

## Date and signatures

.....

**00531 Helsinki,**

.....  
(location, date signed)

.....

.....  
(party 35)

P35 AKA  
Academy of Finland  
Hakaniemenranta 6  
00531 Helsinki  
Finland

## Date and signatures

8010 Graz,

.....

.....  
(location, date signed)

.....

.....  
(party 36)

P36   BBMRI-ERIC  
Biobanking an Biomolecular Resources  
Research Infrastructure - European  
Research Infrastructure Consortium  
NEUE STIFTINGTALSTRASSE 2/B/6  
000  
8010 Graz  
Austria

## Date and signatures

.....

**1100 KOBENHAVN K,**

.....  
(location, date signed)

.....

.....  
(party 37)

P37 IFD  
Innovation Fund Denmark  
OSTERGADE 26 A 000  
1100 KOBENHAVN K  
Denmark

## Date and signatures

.....

.....

1077 Budapest,

.....  
(location, date signed)

.....  
(party 38)

P38 NKFIH  
National Research, Development and  
Innovation Office  
KETHLY ANNA TER 1 000  
1077 Budapest  
Hungary

## Date and signatures

.....

.....

**1050 Riga,**

.....  
(location, date signed)

.....  
(party 39)

P39 LCS  
Latvian Council of Science  
SMILSU IELA 8 000  
1050 Riga  
Latvia

## Date and signatures

.....

.....

**3000-069 COIMBRA,**

.....  
(location, date signed)

.....  
(party 41)

P41 CCDRC  
Comissão de Coordenação e  
Desenvolvimento Regional do Centro  
RUA BERNARDIM RIBEIRO 80  
3000-069 COIMBRA  
Portugal

## Date and signatures

**3000-069 COIMBRA,**

.....  
(location, date signed)

.....  
(party 42)

P42 RANNIS  
The Icelandic Centre for Research  
BORGARTUNI 30 000  
105 Reykjavik  
Iceland



## Date and signatures

00153 Roma,

.....

.....  
(location, date signed)

.....

.....  
(party 43)

P43 MUR  
Ministry of Economy and Finance  
Revolving Fund Community Policies  
Via Michele Carcani 61  
00153 Roma  
Italy

## Date and signatures

**01010 Vitoria-Gasteiz,**

.....

.....  
(location, date signed)

.....

.....  
(party 44)

P44 DPTO Salud  
DEPARTAMENTO DE SALUD  
GOBIERNO VASCO  
Donostia-San Sebastián, 1  
01010 Vitoria-Gasteiz  
Spain

.....

.....  
(party 44.1)

P44.1 BIOEF  
Department of Health and the Basque  
Foundation for Health Research and  
Innovation (BIOEF)

Spain

## Date and signatures

010362 Bucuresti,

.....  
(location, date signed)

.....  
(party 45)

P45 UEFISCDI  
UNITATEA EXECUTIVA PENTRU  
FINANTAREA INVATAMANTULUI  
SUPERIOR A CERCETARII  
DEZVOLTARII SI INOVARII  
STR D I MENDELEEV 21-25 000  
010362 Bucuresti  
Romania

## Date and signatures

**53123 Bonn,**

.....

.....  
(location, date signed)

.....

.....  
(party 46)

P46    BMG  
Federal Ministry of Health  
Rochustr. 1  
53123 Bonn  
Germany

## Date and signatures

**53175 Bonn,**

.....

.....  
(location, date signed)

.....

.....  
(party 47)

P47 BMBF  
Bundesministerium für Bildung und  
Forschung  
Heinemannstr. 2  
53175 Bonn  
Germany

## Date and signatures

**1010 Wien,**

.....

.....  
(location, date signed)

.....

.....  
(party 48)

P48 BMBWF  
Bundesministerium für Bildung,  
Wissenschaft und Forschung  
MINORITENPLATZ 5  
1010 Wien  
Austria

## Date and signatures

**1030 Bruxelles,**

.....

.....  
(location, date signed)

.....

.....  
(party 49)

P49 FIO  
FONDS INNOVEREN EN  
ONDERNEMEN  
BOULEVARD DU ROI ALBERT II 35 12  
1030 Bruxelles  
Belgium

## Date and signatures

**3003 Bern,**

.....

.....  
(location, date signed)

.....

.....  
(party 50)

P50 INNOSUISSE  
INNOSUISSE  
EINSTEINSTRASSE 2; po box: 000  
3003 Bern  
Switzerland



## **Annex 1 - Responsibilities of the parties (in accordance with Section 3 of this agreement)**

The base of activities as well as responsibilities executed within EP PerMed is the description of actions in the Grant Agreement. In the following tables the data processing tools used in EP PerMed processing activities and appointment of responsibilities within EP PerMed are described

### **Tools and platforms used for the processing of personal data:**

<b>General processing platform</b>	<b>Categories of personal data</b>	<b>Means of processing</b>	<b>Who is responsible for data collection and processing?</b>	<b>Recipients/Categories of recipients/processors</b>
Email server used by joint controllers for processing emails with personal data content	Dependent on content in email	encrypted email	Respective joint controller using email server	Staff of joint controllers
<b>EP PerMed sharepoint</b>	Various (e.g. list of EP PerMed consortium members, list of stakeholders, attendance lists of meetings)	Secured online storage and secured computers	DLR is responsible for the set-up and maintenance of the sharepoint, joint controllers are responsible for uploading and management of data	Staff of joint controllers
<b>PT-Outline</b>	Various (e.g. name, email addresses of applicants and reviewers, unpublished scientific content)	Secured online storage and secured computers	DLR is responsible for the set-up and maintenance of and data security in PT-Outline, the respective Joint Call Secretariats are responsible for their downloads of the data that will be asked from applicants and reviewers (necessary for call management)	Staff of DLR and staff of Joint Call Secretariats
<b>Registration tool (e.g. Invitatio)</b>	Name, function, email address, contact details, other types of	Secured online storage and	Respective joint controller setting up the registration tool	Staff of respective joint controllers

	personal data (e.g. bank data for travel reimbursement)	secured computers		
<b>Survey tools (tbd)</b>	Name, function, email address, contact details, survey answers related to personalised medicine	Secured online storage and secured computers	Respective joint controller responsible for setting up the survey	Staff of respective joint controllers
<b>Partnering tool (hosted by DLR)</b>	Name, function, email address, contact details	Secured online storage and secured computers	DLR	No data transfer planned
<b>Newsletter</b>	Name, email address,	Secured online storage and secured computers	DLR	No data transfer planned
<b>Access Mapping Database</b>	Name, email address,	Secured online storage and secured computers	DLR	No data transfer planned

**Description of the processing activities of personal data:**

<b>Categories of data subjects</b>	<b>Categories of personal data</b>	<b>Purpose of processing</b>	<b>Means of processing</b>	<b>Who is responsible for data collection, processing and storage?</b>	<b>Recipients/ Categories of recipients</b>
<b>Employees of the Funding Organisation s participating in the EP PerMed activities and Joint Transnational Calls</b>	General data, professional data	Main purposes pursued: <ul style="list-style-type: none"><li>• Implementatio n of joint activities of EEP PerMed, including the Joint Transnational Calls.</li></ul>	<u>Means of collection:</u>  Encrypted emails and EP PerMed Sharepoint <u>Processing through:</u>  Excel files; EP PerMed Sharepoint <u>Storage:</u>  Secured email	<u>Collection:</u> All Joint Call Secretariats participants, the work package and task leaders responsible of the organisation of the different EP PerMed activities	Staff of Joint Controllers

		<ul style="list-style-type: none"> <li>• Internal communication</li> <li>•</li> </ul>	servers, EP PerMed Sharepoint; online storage and secured computers.	<p><u>Processing:</u> each Joint Controller.</p> <p><u>Storage:</u> DLR (for sharepoint), each Joint Controller</p>	
<b>Coordinators and team members in submitted proposals</b>	General data, professional data, unpublished research results, contractual data, other.	<p>The data of the applicants is used to ensure a proper evaluation process in the call for proposals launched by EP PerMed , namely:</p> <ul style="list-style-type: none"> <li>• to communicate about the application process and results of the call,</li> <li>• to allow participating funding organisations to perform an eligibility check of the applicants,</li> <li>• to evaluate the proposals and consortia (by external reviewers),</li> </ul> <p>To share the evaluation results of the proposals with the Call Steering Committee and the external observers.</p>	<p><u>Means of collection:</u> Submission of application forms through PT-Outline. Consent of the researchers to process their data will be collected via the PT-Outline</p> <p><u>Processing through</u> Excel files gathering all the information, circulation among CSC members via encrypted Email, EP PerMed Sharepoint</p> <p>Direct access to PT-Outline for the evaluators will be organised by each Joint Call Secretariat</p> <p><u>Storage</u> Stored on the pt-outline, secured online storage and in</p>	<p><u>Collection:</u> DLR (for PT-Outline), Joint Call Secretariats</p> <p><u>Processing:</u> Each Controller will process personal data of its national applicants. JCS, Call Steering Committee and external reviewers will process personal data of all the applicants.</p> <p><u>Storage:</u> DLR (for PT-Outline), Joint Call Secretariat (for downloaded data), each controller for data forwarded via email</p>	All Joint Controllers; external reviewers (data transfer will be regulated via an additional agreement, e.g. declaration of conflict of interest, non-disclosure agreement))

		<ul style="list-style-type: none"> <li>•to award funding if the application is successful,</li> <li>•to perform analysis on the submitted proposals</li> </ul>	secured computers.		
<b>Coordinators and team members in financed projects</b>	General data, professional data, contractual data, other.	<p>Personal data of the selected researchers is needed to:</p> <ul style="list-style-type: none"> <li>• communicate with the Researchers selected for funding about their awarded project,</li> <li>• allow funding organisation to contact the selected applicants to elaborate funding contracts,</li> <li>• organise follow-up events, including net-working workshops,</li> <li>• perform monitoring and evaluation of the funded projects,</li> <li>• develop brochures pre-senting the selected projects and their outputs,</li> </ul>	<p><u>Means of collection</u></p> <p>Submission of application forms through the pt-outline, e-mails, Excel files. During the application process, it is requested the consent of the researchers to process their data collected on the pt-outline, specifying the set of general data that they consent to make publicly available.</p> <p><u>Processing through:</u></p> <p>Excel files gathering all the information.</p> <p><u>Storage:</u></p> <p>Stored in secured online storage and secured computers.</p>	<p>Collection: Joint Call Secretariat, Call Steering Committee.</p> <p>Processing: Joint Call Secretariat, Call Steering Committee, all Joint Controllers.</p> <p>Storage: Joint Call Secretariat, Call Steering Committee</p>	All Joint Controllers

		Present and disseminate public statistics of the Joint Transnational Calls			
<b>External Reviewers of proposals (including International Peer Review Panel members)</b>	General data, professional data, contractual data, other types of personal data (e.g. bank data for travel reimbursement); non-disclosure agreements, conflict of interests	<p>The data of the external reviewers is used to:</p> <ul style="list-style-type: none"> <li>• Select and invite the most qualified Peer Review Panel members to evaluate the proposals of a Call,</li> <li>• Communicate with the members of the Peer Review Panel,</li> <li>• Assign them applications to review,</li> <li>• Collect their evaluation,</li> <li>• Organise the Peer Review Panel meeting (e.g. travels, travel reimbursement),</li> </ul>	<p><u>Means of collection:</u></p> <p>Excel-lists with suggested reviewers from Joint Call Secretariat, Call Steering Committee members, and emails</p> <p><u>Processing through:</u></p> <p>Evaluation of the relevance of their profiles to evaluate project proposals on the pt-outline platform. Excel files gathering all the information and forms completed by the Peer Review Panel members – pt-outline: Peer Review Panel Members give a formal consent on the collection of their data on the pt-outline, a declaration about conflict of interests and a non-</p>	<p><u>Collection:</u></p> <p>All Joint Controllers may provide the Joint Call Secretariat with Personal data of potential Peer Review Panel members and obtain information on the Peer Review Panel members via encrypted emails. Most of the collection of these personal data will be realised by the Joint Call Secretariat of an individual Joint Transnational Call.</p> <p><u>Processing:</u></p> <p>DLR-PT for PT-Outline, Joint Call Secretariats, Call Steering Committee</p> <p>Other types of personal data (e.g. bank data for travel reimbursement) will only be collected, processed</p>	All Joint Controllers.

			disclosure agreement. <u>Storage:</u> Secured online storage and secured computers.	and stored by those Joint Controllers that need them for performing specific tasks. <u>Storage:</u> DLR (for PT-Outline), Joint Call Secretariat (for downloaded data), each controller for data forwarded via email	
<b>Members of advisory bodies in EP PerMed (including: EP PerMed Advisory Board, Call Advisory Board, Innovation Advisory Board, ICPerMed Advisory Board, Working Groups and Stakeholder Forum )</b>	General data, professional data, contractual data, other types of personal data (e.g. bank data for travel reimbursement).	Main purposes pursued: <ul style="list-style-type: none"><li>• Communication with the members of the advisory bodies in EP PerMed for the different activities in which they will be involved</li><li>• Organisation of advisory bodies meetings, travels &amp; reimbursement procedures</li></ul>	<u>Means of collection:</u> Joint Controllers responsible of the establishment of each advisory board. Consent of the members of the advisory bodies to process their data collected and signature of the confidential disclosure agreement  <u>Processing through</u> Excel files gathering all the information.  <u>Storage:</u>	<u>Collection:</u> Joint Controllers responsible of the establishment of each advisory board.  <u>Processing:</u> Joint Data Controllers responsible of the establishment of each advisory board and the organisation of the meetings of those advisory boards.  Other types of personal data (e.g. bank data for travel reimbursement) will only be	All Joint Controllers

			Stored in secured computers and secured online storage	collected, processed and stored by those Joint Controllers that need them for performing specific tasks.  Storage:  Joint controller in charge of the organisation of the advisory board meetings	
<b>Guests/speakers at events/observers/stakeholders</b>	General data, professional data, contractual data, other types of personal data (e.g. bank data for travel reimbursement plus photos.	<p>Main purposes pursued:</p> <ul style="list-style-type: none"> <li>• Organisation of the events, travels &amp; reimbursement procedures</li> </ul> <p>Contact for joint publications, organisations of events.</p>	<p><u>Means of collection:</u></p> <p>Joint Controllers responsible of the organisation of the events or joint activity/publication will collect the information through registration forms, emails, internet research etc.</p> <p><u>Processing through</u></p> <p>Excel files gathering all the information. Other type of documents or registration tools.</p> <p><u>Storage:</u></p>	<p><u>Collection:</u></p> <p>Joint Controllers responsible of the organisation of the events and joint activities with stakeholders.</p> <p><u>Processing:</u></p> <p>Joint Data Controllers responsible of the organisation of the events and joint activities with stakeholders.</p> <p>Other types of personal data (e.g. bank data for travel reimbursement, photos) will only be collected, processed and storage by those Joint</p>	All Joint Controllers

			Stored in secured computers	Controllers that need them for performing specific tasks.  Storage:  Joint controller in charge of the organisation of the events or the joint activities with stakeholders	
<b>Event participants</b>	General data, professional data, other types of personal data (e.g. bank data for travel reimbursement) plus photos	Main purposes pursued:  • Organisation of the events	<u>Means of collection:</u>  Joint Controllers responsible of the organisation of the events will collect the information through registration forms, emails, etc. Consent of the participants of the events to process their data collected.  <u>Processing through</u>  Excel files gathering all the information. Other type of documents or registration tools.  <u>Storage:</u> Stored in secured computers	<u>Collection:</u>  Joint Controllers responsible of the organisation of the events.  <u>Processing:</u>  Joint Controllers responsible of the organisation of the events.  Storage:  Joint controller in charge of the organisation of the respective event	All Joint Controllers



			and secured online storage		
<b>EP PerMed newsletter recipients</b>	General data	<p>Main purposes pursued:</p> <ul style="list-style-type: none"> <li>• Newsletter dissemination</li> </ul>	<p><u>Means of collection:</u></p> <p>DLR will collect the information through registration forms. Consent of the recipients of the newsletter to process their data will be collected.</p> <p><u>Processing through</u></p> <p>Excel files gathering all the information. Other type of documents or registration tools.</p> <p><u>Storage:</u></p> <p>Stored in secured computers and secured online storage</p>	<p><u>Collection:</u></p> <p>DLR responsible of the dissemination of the newsletter.</p> <p><u>Processing:</u></p> <p>DLR responsible of the dissemination of the newsletter.</p> <p><u>Storage:</u></p> <p>DLR responsible of the dissemination of the newsletter.</p>	No data transfer planned
Partnering Tool	General data	<p>Main purposes pursued:</p> <ul style="list-style-type: none"> <li>• Create a contact point for researchers to find partners for EP PerMed Calls</li> </ul>	<p><u>Means of collection:</u></p> <p>DLR will collect the information through registration forms. Consent of the recipients of the partnering tool to process</p>	<p><u>Collection:</u></p> <p>DLR responsible of the partnering tool.</p> <p><u>Processing:</u></p> <p>DLR responsible of the partnering tool.</p> <p><u>Storage:</u></p>	No data transfer planned

			<p>their data will be collected.</p> <p><u>Processing through</u></p> <p>Excel files gathering all the information. Other type of documents or registration tools.</p> <p><u>Storage:</u> Stored in secured computers and secured online storage</p>	<p>DLR responsible of the partnering tool.</p>	
<p><b>Registrants to access to Mapping Database</b></p>	<p>General data</p>	<p>Main purposes pursued:</p> <ul style="list-style-type: none"> <li>• provide information about national and regional funding activities in personalised medicine</li> </ul>	<p><u>Means of collection:</u></p> <p>DLR will collect the information through registration forms. Consent of the registrants for access of the mapping database to process their data will be collected.</p> <p><u>Processing through</u></p> <p>Excel files gathering all the information. Other type of documents or registration tools.</p> <p><u>Storage:</u> Stored in</p>	<p><u>Collection:</u></p> <p>DLR responsible of the partnering tool.</p> <p><u>Processing:</u></p> <p>DLR responsible of the Mapping Database</p> <p><u>Storage:</u></p> <p>DLR responsible of the Mapping Database</p>	<p>All Joint Controllers</p>

			secured computers and secured online storage		
<b>Survey participants</b>	General data, professional data, answers to survey questions	Main purposes pursued: <ul style="list-style-type: none"> <li>• increase knowledge base in personalised medicine</li> </ul>	<u>Means of collection:</u>  <u>Joint Controllers responsible of the organisation of the survey will collect the information through registration forms, emails, etc. Consent of the participants of the events to process their data collected. Subcontracting is possible but not yet determined.</u>  <u>Processing through</u>  <u>Excel files gathering all the information. Other type of documents or registration tools.</u>  <u>Storage:</u> <u>Stored in secured computers and secured online storage</u>	<u>Collection:</u> Joint Controllers responsible of the organisation of the survey.  <u>Processing:</u> Joint Controllers responsible of the organisation of the survey.  <u>Storage:</u> Joint controller in charge of the organisation of the respective survey	All Joint Controllers

## **Annex 2 - subcontractor**

The following entities shall be approved subcontractors within the meaning of Section 11:

### A.) List of subcontractors used by DLR

<b>company name</b>	<b>location of service / main establishment</b>	<b>Scope of services</b>
TEDSoft GmbH	Friedrich-Breuer-Str. 118 53225 Bonn	Programming partnering tool
HOSTPRESS	Bahnhofstraße 34 66571 Eppelborn	EP PerMed webpage hosting
Invitario GmbH	Lohmühlenstraße 65 12435 Berlin	Event registration

### **Annex 3 – List of contact persons**

1. DEUTSCHES ZENTRUM FÜR LUFT - UND RAUMFAHRT EV – DLR established in LINDER HOHE, 51147, KOLN, DE // DPO Contact: Uwe Gorschütz, e-mail: [datenschutz@dlr.de](mailto:datenschutz@dlr.de) Website: <https://www.dlr.de>
2. AGENCE NATIONALE DE LA RECHERCHE – ANR, established in 86 RUE REGNAULT, 75013, PARIS, FR // DPO Contact: Véronique Pauliac // <https://anr.fr/fr/rgpd/>
3. VLAAMSE GEWEST - VL O, established in AVENUE DU PORT 88, 1000, BRUSSEL, BE DPO Contact: Zoë De Ruyck, e-mail: [dpo.ewi@vlaanderen.be](mailto:dpo.ewi@vlaanderen.be)
4. INSTITUTO ARAGONES DE CIENCIAS DE LA SALUD – IACS, established in AVENIDA SAN JUAN BOSCO 13, 50009, ZARAGOZA, ES // DPO Contact: e-mail: [protecciondatos.iacs@aragon.es](mailto:protecciondatos.iacs@aragon.es)
5. FONDAZIONE TOSCANA LIFE SCIENCES – TLS, established in VIA FIORENTINA 1, 53100, SIENA, IT // DPO Contact: Avv. Claudia del Re, e-mail: [dpo@toscanalifesciences.org](mailto:dpo@toscanalifesciences.org)
6. NORGES FORSKNINGSRAD - THE RESEARCH COUNCIL OF NORWAY, established in DRAMMENSVEIEN 288, 0283, OSLO, NO //DPO Contact: e-mail: [personvern@forskningsradet.no](mailto:personvern@forskningsradet.no)
7. MINISTERO DELLA SALUTE – IT MoH, established in Via Giorgio Ribotta 5, 00144, ROMA, IT //DPO Contact: Benini Massimiliano, e-mail: [m.benini@sanita.it](mailto:m.benini@sanita.it)
8. INSTITUTO DE SALUD CARLOS III – ISCIII, established in MONFORTE DE LEMOS 5, 28029, MADRID, ES// DPO Contact: Ana Ibañez, e-mail: [dpd@isciii.es](mailto:dpd@isciii.es); [protecciondatos@isciii.es](mailto:protecciondatos@isciii.es)
9. SCIENCE FOUNDATION IRELAND – SFI, established in THREE PARK PLACE, HATCH STREET UPPER, D002FX65, DUBLIN, IE //DPO Contact: Elliot McVann, e-mail: [elliot.mcvann@sfi.ie](mailto:elliot.mcvann@sfi.ie); [sfidataprivacy@sfi.ie](mailto:sfidataprivacy@sfi.ie)
10. SAECHSISCHES STAATSMINISTERIUM FÜR WISSENSCHAFT, KULTUR UND TOURISMUS – SMWK, established in WIGARDSTRASSE 17, 01097, Dresden, DE // DPO Contact: e-mail: [dsb@smwk.sachsen.de](mailto:dsb@smwk.sachsen.de)
11. FONDAZIONE TELETHON ETS - FONDAZIONE TELETHON ETS, established in VIA VARESE 16/B, 00185, ROMA, IT // DPO Contact: Michela Maggi, e-mail: [mmaggi@maggilegal.it](mailto:mmaggi@maggilegal.it); [michela.maggi@milano.pecavvocati.it](mailto:michela.maggi@milano.pecavvocati.it)
12. FONDAZIONE REGIONALE PER LA RICERCA BIOMEDICA – FRRB, established in PIAZZA CITTA DI LOMBARDIA 1, 20124, MILANO, IT //DPO Contact: Ivano Pecis, e-mail: [privacy@frrb.it](mailto:privacy@frrb.it); [dpo.frrb@pec.it](mailto:dpo.frrb@pec.it)
13. FONDS ZUR FÖRDERUNG DER WISSENSCHAFTLICHEN FORSCHUNG – FWF, established in GEORG-COCH-PLATZ 2, 1010, WIEN, AT // DPO Contact: Elvise Seumenicht, e-mail: [Elvise.Seumenicht@fwf.ac.at](mailto:Elvise.Seumenicht@fwf.ac.at)
14. THE HEALTH RESEARCH BOARD – HRB, established in 67 72 LOWER MOUNT STREET, D02 H638, DUBLIN, IE //DPO Contact: Martin Morgan, e-mail: [mmorgan@hrb.ie](mailto:mmorgan@hrb.ie)
15. Lietuvos mokslo taryba – LMT, established in Gedimino 3, LT-01103, Vilnius, LT // DPO Contact: Marius Dijokas, e-mail: [dap@lmt.lt](mailto:dap@lmt.lt) \_website: <https://lmt.lrv.lt/en/>
16. MINISTRY OF HEALTH - CSO-MOH, established in YIRMIYAHU 39, 9101002, JERUSALEM, IL // DPO Contact: Reuven Eliahu, e-mail: [reuven.eliahu@MOH.GOV.IL](mailto:reuven.eliahu@MOH.GOV.IL)
17. SIHTASUTUS EESTI TEADUSAGENTUUR – ETAg, established in SOOLA 8, 51004, TARTU, EE // DPO Contact: Kati Uusmaa \_e-mail: [kati.uusmaa@etag.ee](mailto:kati.uusmaa@etag.ee)

18. TURKIYE BILIMSEL VE TEKNOLOJIK ARASTIRMA KURUMU – TUBITAK, established in Ataturk Bulvari no 80, 06100, ANKARA, TR // DPO Contact: Rafet Öngöçmen\_e-mail: rafet.ongocmen@tubitak.gov.tr
19. EIT HEALTH EV, established in MIES-VAN-DER-ROHE-STRASSE 1 C, 80807, MUNCHEN, DE // DPO Contact: e-mail: DataPrivacy@eithealth.eu
20. VERKET FOR INNOVATIONSSYSTEM - VINNOVA SWEDISH AGENCY FOR INNOVATION SYSTEMS – VINNOVA, established in MASTER SAMUELSG 56, 10158, STOCKHOLM, SE // DPO Contact: e-mail: dataskyddsbud@vinnova.se
21. NARODOWE CENTRUM BADAN I ROZWOJU – NCBR, established in UL. CHMIELNA 69, 00-801, WARSZAWA, PL // DPO Contact: Ewa Chrzanowska\_e-mail: iod(@)lodzkie.straz.gov.pl
22. AGENCIA DE INVESTIGACAO CLINICA E INOVACAO BIOMEDICA – AICIB, established in RUA DE SANTA CATARINA 1288, 4000-447, PORTO, PT // DPO Contact: Maria Rita Pais de Vasconcelos Pereira Coutinho\_e-mail: privacy@aicib.pt
23. FUNDACAO PARA A CIENCIA E A TECNOLOGIA – FCT, established in AVENIDA D CARLOS I 126, 1249 074, LISBOA, PT // DPO Contact: Margarida Vaz\_e-mail: dpo@fct.pt
24. ZORGONDERZOEK NEDERLAND ZON – ZON, established in Laan Van Nieuw Oost Indie 334, 2593 CE, DEN HAAG, NL // DPO Contact: Lennart Huizing\_e-mail: privacy@zonmw.nl
25. FONDS NATIONAL DE LA RECHERCHE – FNR, established in 2 AVENUE DE L'UNIVERSITE, 4365, ESCH-SUR-ALZETTE, LU // DPO Contact: MGSi sarl, Ms Gagnon\_e-mail: info@mgsi.lu
26. REGIONE TOSCANA – RT, established in Palazzo Strozzi Sacratì - Piazza del Duomo 10, 50122, FIRENZE, IT // DPO Contact: Filippo Castagna\_e-mail: urp\_dpo@regione.toscana.it
27. SERVICE PUBLIC DE WALLONIE – SPW, established in Place de la Wallonie 1, 5100, Namur, BE // DPO Contact: e-mail: securite.eer@spw.wallonie.be
28. FONDS DE LA RECHERCHE SCIENTIFIQUE- FNRS, established in RUE D'EGMONT 5, 1000, BRUXELLES, BE // DPO Contact: Ada Stone SRL\_e-mail: privacy.fnrs@adastone.law
29. DEPARTAMENT DE SALUT - GENERALITAT DE CATALUNYA – DS CAT, established in Trav. de les Corts (Pavelló Ave Maria) 131-159, 08028, BARCELONA, ES // DPO Contact: Carme Pérez\_e-mail: Carme Pérez peris@gencat.cat
30. COMUNIDAD FORAL DE NAVARRA - GOBIERNO DE NAVARRA - COMUNIDAD FORAL DE NAVARRA – CFN, established in AVENIDA CARLOS III 2, 31002, PAMPLONA, ES // DPO Contact: Unidad Delegada de Protección de Datos del Gobierno de Navarra\_e-mail: dpd@navarra.es
31. SOTSIAALMINISTEERIUM – MSAE, established in Suur-Ameerika 1, 10122, TALLINN, EE // DPO Contact: Lily Mals\_e-mail: Lily.mals@sm.ee
32. FONDS VOOR WETENSCHAPPELIJK ONDERZOEK-VLAANDEREN - FWO, established in LEUVENSEWEG 38, 1000, BRUSSEL, BE // DPO Contact: Jasper Feliersj\_e-mail: Jasper.Feliers@fwo.be
33. INNOVAATIO RAHOITUSKESKUS BUSINESS FINLAND – BFRK, established in PO BOX 69, 00101, HELSINKI, FI // DPO Contact: Maija-Liisa Pykkänen\_e-mail: data.protection@businessfinland.fi
34. VETENSKAPSRÅDET - SWEDISH RESEARCH COUNCIL – SRC, established in BOX 1035, 101 38, STOCKHOLM, SE // DPO Contact: Per Bergstrand\_e-mail: dataskyddsbudet@vr.se

35. SUOMEN AKATEMIA – AKA, established in HAKANIEMENRANTA 6, 00531, HELSINKI, FI // DPO Contact: Laura Kuitunen\_e-mail: laura.kuitunen@aka.fi
36. BIOBANKS AND BIOMOLECULAR RESOURCES RESEARCH INFRASTRUCTURE CONSORTIUM (BBMRI-ERIC) - BBMRI-ERIC, established in NEUE STIFTINGTALSTRASSE 2/B/6, 8010, GRAZ, AT // DPO Contact: Erdina Ene\_e-mail: dpo@bbmri-eric.eu
37. INNOVATIONSFONDEN - DANMARK INNOVATIONSFOND DANISH INNOVATION FOUNDATION – IFD, established in OSTERGADE 26 A, 1100, KOBENHAVN K, DK // DPO Contact: Nadia Holdgaard Krog\_e-mail: nadia.holdgaard.krog@innofond.dk
38. NEMZETI KUTATASI FEJLESZTESI ES INNOVACIOS HIVATAL – NKFIH, established in KETHLY ANNA TER 1, 1077, BUDAPEST, HU // DPO Contact: Dr. Csaba Gyula Górá\_e-mail: adatvedelmitisztviselo@nkfi.gov.hu
39. LATVIJAS ZINATNES PADOME – LZP, established in SMILSU IELA 8, 1050, RIGA, LV // DPO Contact: Jevgeņijs Jarosovs\_e-mail: das@idagentura.lv; pasts@lzp.gov.lv
40. VICE-PRESIDENCIA DO GOVERNO REGIONAL DOS AÇORES – VP GRA, established in LARGO PRIOR DO CRATO, 9700-157, ANGRA DO HEROÍSMO, PT // DPO Contact: e-mail: epd-vpgr@azores.gov.pt
41. COMISSAO DE COORDENACAO E DESENVOLVIMENTO REGIONAL DO CENTRO – CCDRC, established in RUA BERNARDIM RIBEIRO 80, 3000-069, COIMBRA, PT // DPO Contact: e-mail: geral@ccdrc.pt
42. RANNSOKNAMIDSTOD ISLANDS – Rannis, established in BORGARTUNI 30, 105, REYKJAVIK, IS // DPO Contact: Elísabet M. Andrésdóttir\_website: <https://www.rannis.is>
43. Ministero dell'università e della ricerca – MUR, established in Via Michele Carcani 61, 00153, Roma, IT // DPO Contact: e-mail: rpd@mur.gov.it
44. DEPARTAMENTO DE SALUD GOBIERNO VASCO – DPTO SALUD, established in Donostia-San Sebastián, 1, 01010, VITORIA-GASTEIZ, ES // DPO Contact: website: <https://www.euskadi.eus>
45. UNITATEA EXECUTIVA PENTRU FINANTAREA INVATAMANTULUI SUPERIOR A CERCETARII DEZVOLTARII SI INOVARII – UEFISCDI, established in STR D I MENDELEEV 21-25, 010362, BUCURESTI, RO // DPO Contact: Victor Velter\_e-mail: protectiadatelor@uefiscdi.ro
46. BUNDESMINISTERIUM FUER GESUNDHEIT – BMG, established in ROCHUSTRASSE 1, 53123, BONN, DE // DPO Contact: e-mail: DSB(at)bmg.bund.de
47. BUNDESMINISTERIUM FUER BILDUNG UND FORSCHUNG – BMBF, established in Heinemannstrasse 2, 53175, BONN, DE // DPO Contact: e-mail: datenschutz@bmbf.bund.de
48. BUNDESMINISTERIUM FUER BILDUNG, WISSENSCHAFT UND FORSCHUNG – BMBWF, established in MINORITENPLATZ 5, 1010, VIENNA, AT // DPO Contact: Lothar Hahn\_e-mail: Lothar.hahn@bmbwf.gv.at
49. FONDS INNOVEREN EN ONDERNEMEN – HERMESFOND – FIO, established in BOULEVARD DU ROI ALBERT II 35, 1030, BRUXELLES, BE // DPO Contact: Bart Grieten\_e-mail: dpo@vlaio.be
50. SWISS INNOVATION AGENCY – INNOSUISSE, established in EINSTEINSTRASSE 2, 3003 BERN, CH // DPO Contact: e-mail: legal@innosuisse.ch

**Annex 4 - Appropriate safeguards for third country transfers in accordance with Articles 44 to 49 GDPR**

**STANDARD CONTRACTUAL CLAUSES<sup>1</sup>**

**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)<sup>2</sup> 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.

---

<sup>1</sup> Brussels, 04/06/2021/ C(2021) 3972 final

<sup>2</sup> Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision [...].



## *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 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
  - (iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
  - (iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
  - (v) Clause 13;
  - (vi) Clause 15.1(c), (d) and (e);
  - (vii) Clause 16(e);
  - (viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
- (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*

##### ***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.

#### **MODULE ONE: Transfer controller to controller**

##### **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<sup>3</sup> 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

---

<sup>3</sup> 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.

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<sup>4</sup> (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**

---

<sup>4</sup> 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.

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 10*

### ***Data subject rights***

#### **MODULE ONE: Transfer controller to controller**

- (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.<sup>5</sup> 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

---

<sup>5</sup> 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.

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 lay 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<sup>6</sup> at no cost to the data subject. It shall

---

<sup>6</sup> 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.



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.]

#### **MODULE ONE: Transfer controller to controller**

- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

#### *Clause 12*

#### ***Liability***

#### **MODULE ONE: Transfer controller to controller**

- (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***

#### **MODULE ONE: Transfer controller to controller**

- (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***

#### **MODULE ONE: Transfer controller to controller**

- (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<sup>7</sup>;
  - (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.

---

<sup>7</sup> 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.

- (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***

#### **MODULE ONE: Transfer controller to controller**

##### **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.

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

- (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.). [For Module Three: The data exporter shall forward the information to the controller.]
- (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. [For Module Three: The data exporter shall make the assessment available to the controller.]

- (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 [for Module Three: and the controller] 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) [For Modules One, Two and Three: 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.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] 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***

#### **MODULE ONE: Transfer controller to controller**

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 Germany.

#### *Clause 18*

#### ***Choice of forum and jurisdiction***

#### **MODULE ONE: Transfer controller to controller**

- (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 Germany.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

## **APPENDIX**

### **EXPLANATORY NOTE:**

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

## **ANNEX I**

### **A. LIST OF PARTIES**

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

**1. Name: DLR Projekttraeger (DLR)** (as coordinator of EP PerMed)

- Address: Heinrich-Konen-Str. 1, 53227 Bonn, Germany
- Contact person's name, position and contact details: Uwe Gorschütz, DPO, [uwe.gorschuetz@dlr.de](mailto:uwe.gorschuetz@dlr.de); [datenschutz@dlr.de](mailto:datenschutz@dlr.de)
- Activities relevant to the data transferred under these clauses: Specified in the Joint Controller Agreement and Appendix 1
- Signature and date: see signature sheet of DLR of this Joint Controller Agreement
- Role (controller/processor): controller

**2. Name: Agence Nationale de la Recherche (ANR)**

- Address: 86 RUE REGNAULT, 75013, PARIS, FRANCE
- Contact person's name, position and contact details: Veronique Pauliac, DPO, <https://anr.fr/fr/rgpd>
- Activities relevant to the data transferred under these clauses: Specified in the Joint Controller Agreement and Appendix 1
- Signature and date: see signature sheet of ANR of this Joint Controller Agreement
- Role (controller/processor): controller



3. Name: **INSTITUTO DE SALUD CARLOS III (ISCIII)**

- Address: Av. Monforte de Lemos, 5, MADRID 28029, Spain,
- Contact person's name, position and contact details: Ana Ibañez, DPO: dpd@isciii.es; protecciondatos@isciii.es
- Activities relevant to the data transferred under these Clauses: Specified in the Joint Controller Agreement and the Appendix 1
- Signature and date: see signature sheet of Instituto de Salud Carlos III (ISCIII) of this Joint Controller Agreement
- Role (controller/processor): controller

4. Name: **ZORGONDERZOEK NEDERLAND ZON**

- Address: Laan Van Nieuw Oost Indie 334, 2593 CE, DEN HAAG, NL
- Contact person's name, position and contact details: Lennart Huizing\_e-mail: privacy@zonmw.nl
- Activities relevant to the data transferred under these Clauses: Specified in the Joint Controller Agreement and the Appendix 1
- Signature and date: see signature sheet of ZORGONDERZOEK NEDERLAND ZON of this Joint Controller Agreement
- Role (controller/processor): controller

5. Name: **EIT HEALTH EV**

- Address: MIES-VAN-DER-ROHE-STRASSE 1 C, 80807, MUNCHEN, DE
- Contact person's name, position and contact details: DataPrivacy@eithealth.eu
- Activities relevant to the data transferred under these Clauses: Specified in the Joint Controller Agreement and the Appendix 1
- Signature and date: see signature sheet of EITH HEATH EV of this Joint Controller Agreement
- Role (controller/processor): controller

6. Name: **VLAAMSE GEWEST**

- Address: AVENUE DU PORT 88, 1000, BRUSSEL, BE
- Contact person's name, position and contact details: Zoë De Ruyck, e-mail: dpo.ewi@vlaanderen.be
- Activities relevant to the data transferred under these Clauses: Specified in the Joint Controller Agreement and the Appendix 1
- Signature and date: see signature sheet of Vlaamse Gewest of this Joint Controller Agreement
- Role (controller/processor): controller

7. Name: **VERKET FOR INNOVATIONSSYSTEM**

- Address: MASTER SAMUELSG 56, 10158, STOCKHOLM, SE
- Contact person's name, position and contact details: e-mail: dataskyddsbud@vinnova.se
- Activities relevant to the data transferred under these Clauses: Specified in the Joint Controller Agreement and the Appendix 1
- Signature and date: see signature sheet of VERKET FOR INNOVATIONSSYSTEM of this Joint Controller Agreement
- Role (controller/processor): controller

8. Name: **MINISTERO DELLA SALUTE**

- Address: Via Giorgio Ribotta 5, 00144, ROMA, IT
- Contact person's name, position and contact details: Benini Massimiliano, e-mail: m.benini@sanita.it
- Activities relevant to the data transferred under these Clauses: Specified in the Joint Controller Agreement and the Appendix 1
- Signature and date: see signature sheet of MINISTERO DELLA SALUTE of this Joint Controller Agreement
- Role (controller/processor): controller

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

1. Name: **TURKIYE BILIMSEL VE TEKNOLOJIK ARASTIRMA KURUMU (TUBITAK),**

- Address: Ataturk Bulvari 221, ANKARA 06100, Turkiye
- Contact person's name, position and contact details: Rafet Öngöçmen; DPO; email: [rafet.ongocmen@tubitak.gov.tr](mailto:rafet.ongocmen@tubitak.gov.tr)
- Activities relevant to the data transferred under these Clauses: Specified in the Joint Controller Agreement and the Appendix 1
- Signature and date: see signature sheet of TURKIYE BILIMSEL VE TEKNOLOJIK ARASTIRMA KURUMU (TUBITAK) of this Joint Controller Agreement
- Role (controller/processor): controller

2. Name: **The Icelandic Centre for Research**

- Address: BORGARTUNI 30, 105, REYKJAVIK, IS
- Contact person's name, position and contact details: Elísabet M. Andrésdóttir \_website: <https://www.rannis.is>
- Activities relevant to the data transferred under these Clauses: Specified in the Joint Controller Agreement and the Appendix 1
- Signature and date: see signature sheet Icelandic Centre for Research (Rannis) of this Joint Controller Agreement
- Role (controller/processor): controller

3. Name: **MINISTRY OF HEALTH - CSO-MOH**

- Address: YIRMIYAHU 39, 9101002, JERUSALEM, IL
- Contact person's name, position and contact details: Reuven Eliahu, e-mail: reuven.eliahu@MOH.GOV.IL
- Activities relevant to the data transferred under these Clauses: Specified in the Joint Controller Agreement and the Appendix 1
- Signature and date: see signature sheet **MINISTRY OF HEALTH (CSO-MOH)** of this Joint Controller Agreement
- Role (controller/processor): controller

4. Name: **SWISS INNOVATION AGENCY**

- Address: EINSTEINSTRASSE 2, 3003 BERN, CH
- Contact person's name, position and contact details: e-mail: dpo@vlaio.be
- Activities relevant to the data transferred under these Clauses: Specified in the Joint Controller Agreement and the Appendix 1
- Signature and date: see signature sheet **SWISS INNOVATION AGENCY (INNOSUISSE)** of this Joint Controller Agreement
- Role (controller/processor): controller

5. Name: **The Research Council of Norway**

- Address: DRAMMENSVEIEN 288, 0283, OSLO, NO
- Contact person's name, position and contact details: e-mail: personvern@forskningsradet.no
- Activities relevant to the data transferred under these Clauses: Specified in the Joint Controller Agreement and the Appendix 1
- Signature and date: see signature sheet **The Research Council of Norway (RNC)** of this Joint Controller Agreement
- Role (controller/processor): controller

## **B. DESCRIPTION OF TRANSFER**

### **MODULE ONE: Transfer controller to controller**

*Categories of data subjects whose personal data is transferred*

*Described in the Joint Controller Agreement and its Appendix 1*

*Categories of personal data transferred*

*Described in the Joint Controller Agreement and its Appendix 1*

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

*Described in the Joint Controller Agreement and its Appendix 1*

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

*Described in the Joint Controller Agreement and its Appendix 1*

*Nature of the processing*

*Described in the Joint Controller Agreement and its Appendix 1*

*Purpose(s) of the data transfer and further processing*

*Described in the Joint Controller Agreement and its Appendix 1*

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

*Described in the Joint Controller Agreement and its Appendix 1*

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

*Described in the Joint Controller Agreement and its Appendix 1*

## C. COMPETENT SUPERVISORY AUTHORITY

### MODULE ONE: Transfer controller to controller

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

#### Data exporter(s):

##### 1. Name: **DLR Projekttraeger (DLR)**

Competent supervisory authority:

The Federal Commissioner for Data Protection and Freedom of Information

Graurheindorfer Str. 153, 53117 Bonn

Central telephone number: 0228/997799-0

Central e-mail address: [poststelle@bfdi.bund.de](mailto:poststelle@bfdi.bund.de)

Data Protection Officer: Mr. Kapsa

+49228/997799-1950, E-mail address: [bdsb@bfdi.bund.de](mailto:bdsb@bfdi.bund.de)

##### 2. Name: **Agence Nationale de la Recherche (ANR)**

Competent supervisory authority:

L'Autorité de protection des données (APD)

Rue de la Presse 35, 1000 Bruxelles

Telefon: +32 (0) 2 274 48 00

E-Mail: [contact@apd-gba.be](mailto:contact@apd-gba.be)

Homepage: <https://www.datenschutzbehörde.be>

##### 3. Name: **INSTITUTO DE SALUD CARLOS III (ISCIII)**

Competent supervisory authority:

Agencia Española de Protección de Datos (AEPD)

C/Jorge Juan, 6, E - 28001 Madrid

Telefon: + 34 91 266 35 17

E-Mail: [internacional@aepd.es](mailto:internacional@aepd.es)

Homepage: <https://www.agpd.es/>

##### 4. Name: **ZORGONDERZOEK NEDERLAND ZON**

Competent supervisory authority:

Autoriteit Persoonsgegevens

PO Box 93374, 2509 AJ DEN HAAG

Telefon: + 31-70-88 88 500

E-Mail: [internationaal@autoriteitpersoonsgegevens.nl](mailto:internationaal@autoriteitpersoonsgegevens.nl)

Homepage: <https://autoriteitpersoonsgegevens.nl/nl>

5. Name: **EIT HEALTH EV**

Competent supervisory authority:

The Federal Commissioner for Data Protection and Freedom of Information

Graurheindorfer Str. 153, 53117 Bonn

Central telephone number: 0228/997799-0

Central e-mail address: [poststelle@bfdi.bund.de](mailto:poststelle@bfdi.bund.de)

Data Protection Officer: Mr. Kapsa

+49228/997799-1950, E-mail address: [bdsb@bfdi.bund.de](mailto:bdsb@bfdi.bund.de)

6. Name: **VLAAMSE GEWEST**

Competent supervisory authority:

L'Autorité de protection des données (APD)

Rue de la Presse 35, 1000 Bruxelles

Telefon: +32 (0) 2 274 48 00

E-Mail: [contact@apd-gba.be](mailto:contact@apd-gba.be)

Homepage: <https://www.datenschutzbefoeder.be>

7. Name: **VERKET FOR INNOVATIONSSYSTEM**

Competent supervisory authority:

Integritetsskyddsmyndigheten (IMY)

Box 8114, SE-Schweden - 104 20 Stockholm

Telefon: + 46 8 657 6100

E-Mail: [imy@imy.se](mailto:imy@imy.se)

Homepage: [www.imy.se](http://www.imy.se)

8. Name: **MINISTERO DELLA SALUTE**

Competent supervisory authority:

Garante per la Protezione dei Dati Personali

Piazza Venezia n. 11, I - 00187 Roma

Telefon: + 39 06 69 6771

E-Mail: [protocollo@gpdp.it](mailto:protocollo@gpdp.it)

Homepage: <https://www.garanteprivacy.it>

**Data Importer (to be indicated by the Joint Controller):**

**1. Name: TÜRKİYE BİLİMSEL VE TEKNOLOJİK ARASTIRMA KURUMU (TUBITAK)**

Competent supervisory authority:

Personal Data Protection Authority (KVKK)

Nasuh Akar Mahallesi 1407. Sok. No:4, 06520 Çankaya/Ankara

0312 216 50 00

<https://www.kvkk.gov.tr> or <https://sikayet.kvkk.gov.tr>

**2. Name: The Icelandic Centre for Research**

Competent supervisory authority:

Icelandic Data Protection Commissior

Rauðarárstígur 10, 105 Reykjavik, Island

Telefon: +354 5 10 96 00

E-Mail: [postur@personuvernd.is](mailto:postur@personuvernd.is)

<http://www.personuvernd.is/tolvunefnd.nsf/pages/index.html>

**3. Name: Technology Authority, The Government Campus**

9th floor,125 Begin Rd., Tel Aviv, Israel

P.O. Box 7360, Tel Aviv, 61072

Tel.: +972-3-7634050 Fax +972-2-6467064

E-Mail: [ILITA@justice.gov.il](mailto:ILITA@justice.gov.il) <http://www.justice.gov.il/MOJEng/RashutTech/default.html>

**4. Name: SWISS INNOVATION AGENCY**

Competent supervisory authority:

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

Feldeggweg 1, CH - 3003 Bern, Schweiz

Telefon: +41 (0)58 462 43 95

E-Mail: [info@admin.ch](mailto:info@admin.ch) <http://www.edoeb.admin.ch>

**5. Name: The Research Council of Norway**

Competent supervisory authority:

Datatilsynet

Postboks 458 Sentrum, 0105 Oslo, Norwegen

Telefon: + 47 22 39 69 00

E-Mail: [postkasse@datatilsynet.no](mailto:postkasse@datatilsynet.no) <https://www.datatilsynet.no>

## **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.*

*Measures of pseudonymisation and encryption of personal data*

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

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

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

*Measures for user identification and authorisation*

*Measures for the protection of data during transmission*

*Measures for the protection of data during storage*

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

*Measures for ensuring events logging*

*Measures for ensuring system configuration, including default configuration*



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

*Measures for certification/assurance of processes and products*

*Measures for ensuring data minimisation*

*Measures for ensuring data quality*

*Measures for ensuring limited data retention*

*Measures for ensuring accountability*

*Measures for allowing data portability and ensuring erasure*

*For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter*