**DATA TRANSFER AND USE AGREEMENT**

**Colour code:**

Grey background = To be completed;

Yellow background = the internal references to the contract (to be completed or deleted if necessary)

Green background = Guidance through the document, to be deleted at the end.

**Change history**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Nr | Version date | Modified without version change | Description, comments | Control |
| 1.0 | 29.03.2019 |  | Initial DTUA version published | NA |
| 2.0 | 20.11.2020 |  | DTUA V2.0 with included DTPA published; Minimal security requirements included, GDPR compliance considered | JM |
| 3.0 | 01.06.2021 |  | Colour code instructions added; Change history added; I.6 ‘Effective date’ wording changed; IX.3 ‘Counterparts and Electronic form’ wording adapted; III.7 ‘Third party rights’ renamed in ‘Rights of data subjects’; links updated | JM |

✂ **….. Please remove the ‘Colour code instructions’, the green guidance text**

**and the table ‘Change history’ …..** ✂

for the project [#CompleteProjectName]

*The DTUA regulates the conditions under which a data "Provider" (e.g. a hospital) agrees to disclose personal data to a data "Recipient" (e.g. a university). The Provider and the Recipient jointly determine the purpose and means of the processing within the framework of the research project. They both assume the role of "Data Controller" (as opposed to the role of "Data Processor").*

*If the Controllers decide to subcontract the secure transfer and hosting of the data to a third party (the “Processor”), for example to one or more BioMedIT node(s), the relationship between Controllers and Processor has to be regulated in a specific agreement: a Data Transfer and Processing Agreement (DTPA).*

*Note that this agreement should be approved by your legal department, in accordance with the internal rules of your institution.*

This agreement (hereinafter referred to as the “**Agreement**”) is made and entered into by and between:

[name], [address]

and

[name],[address]

[name],[address]

*Add all parties involved: The institutions that are required to exchange data for the project (e.g. University Hospital Basel (USB), Spitalstrasse 21 / Petersgraben 4, CH - 4031 Basel*)

Hereinafter jointly referred to as the “PARTIES” and individually as a “PARTY”;

**WHEREAS**

1. The PARTIES wish to conduct the joint research project \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. A PARTY providing DATA to another PARTY under this Agreement shall be considered a PROVIDER for the purposes of this Agreement. A PARTY receiving DATA from another PARTY under this Agreement shall be considered a RECIPIENT for the purposes of this Agreement.
2. The PROVIDER is the controller of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ data (hereinafter referred to as the “DATA”), as set forth in **Annex I** of this Agreement;
3. The RECIPIENT wishes to conduct the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ research project (hereinafter referred to as the “RESEARCH”), as set forth in **Annex II** of this Agreement, with the DATA made available by the PROVIDER. The PROVIDER is willing to provide such DATA to the RECIPIENT under the terms and conditions as follows hereafter.

**I. Definitions**

Unless defined below, terms shall have the meaning described in the applicable law; in case there is no definition in the law, the SPHN Glossary (<https://sphn.ch/document/sphn-glossary/>) definition shall apply.

*Delete the link, if not applicable*.

For the purpose of this Agreement, capitalized terms, whether used in singular or plural form, shall have the following meaning:

1. **BACKGROUND INTELLECTUAL PROPERTY (BACKGROUND IP)**: shall have the meaning set forth in Section V below.
2. **CODED DATA** or **DATA IN CODED FORM**: means the data linked to a specific person via a code.
3. **CONFIDENTIAL INFORMATION**: means any data, documents or other material (in any form) that is identified as confidential in writing at the time it is disclosed hereunder by a PARTY to its counterpart.
4. **DATA**: means all the data, including the meta data, being transferred (or if not transferred, the data given access to) under this Agreement, as set forth in **Annex I** of this Agreement.
5. **DATA SUBJECT**: means the natural person whose data is processed*.*
6. **EFFECTIVE DATE**: means the date when this Agreement is signed by the duly authorized representatives of two PARTIES, and then for each additional PARTY, the date when the authorized representatives of such PARTY adhere and sign this Agreement.
7. **FOREGROUND INTELLECTUAL PROPERTY (FOREGROUND IP)**: shall have the meaning set forth in Section V below.
8. **INTELLECTUAL PROPERTY RIGHTS:** means all intellectual property rights throughout the world, whether existing under statute, at common law or equity, registered or unregistered, now or hereafter in force or recognized, including trade secrets and know-how.
9. **PROVIDER’S PROJECT LEADER:** means the PROVIDER’s person who takes responsibility for the project as described in the Ordinance on Human Research (**HRO**).
10. **RECIPIENT’S PROJECT LEADER:** means the RECIPIENT’s person who takes responsibility for the project as described in the HRO.
11. **RESEARCH**: means the research project as set forth in **Annex II** of this Agreement, as approved by the Ethics Committee, and for which the DATA will be used;
12. **RESULTS**: means without limitation any output of the RESEARCH such as invention, data, software, algorithms, knowledge, know-how or information that is generated in the RESEARCH, whatever its form or nature, whether or not it can be protected, as well as any rights attached to it, including INTELLECTUAL PROPERTY RIGHTS.

**II. DATA Provision**

1. **Form.** The DATA shall be provided to the RECIPIENT by the PROVIDER in a CODED FORM and in a format to be agreed upon by the PARTIES as per **Annex I.** The RECIPIENT shall not have the key.

*Specify in which form data is provided (uncoded, coded or anonymized).* As a reminder, coded or pseudonymized data is not considered as anonymous data under the Human Research Act.

1. **PROVIDER’s Warranties about DATA Provision** – The PROVIDER warrants that it is entitled to supply the DATA and that all necessary consents and/or authorizations for the transfer and/or use of the DATA to/by the RECIPIENT have been obtained.

*Make sure data provision is made in accordance with the law (e.g. Human Research Act) and your institutional governance processes.*

1. **No PROVIDER’s Warranties about DATA.** It is expressly understood that the PROVIDER does not warrant or guarantee that the DATA will be accurate, complete, or useful for any particular purpose.
2. **No PROVIDER’s Warranties about Third Parties’ INTELLECTUAL PROPERTY RIGHTS.** The PROVIDER offers no warranty that the use of DATA and/or CONFIDENTIAL INFORMATION will not infringe or violate any patent or other proprietary rights of any third party.

**III. DATA Processing**

1. **Purpose**. The RECIPIENT and the RECIPIENT’S PROJECT LEADER agree that the DATA: (a) is to be used only for the academic purposes as described in the RESEARCH plan; (b) may not itself be commercialized, (c) shall not be transferred to or accessed by any third party, for any purposes whatsoever, without the prior written agreement of the PROVIDER and in compliance with the informed consent of the DATA SUBJECT and (d) is only accessed according to the rules as further described in Annex I.

*Note that the purpose may be adapted depending on the project, within the limits of the law.*

1. **Right of use.** The DATA SUBJECT retains her/his right to decide on the use of the DATA provided. The CONFIDENTIAL INFORMATION provided is and remains the property of the PROVIDER.
2. **Security**. The RECIPIENT shall process the DATA in a manner that ensures appropriate security of the DATA, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (‘integrity and confidentiality’), as further described in **Annex III**.

*Refer to appropriate measures, if the recommended ones, as stated above, do not apply. Note that SPHN projects refer to “Ethical Framework for Responsible Data Processing in Personalized Health Research” and in the “SPHN Information Security Policy”, as both updated occasionally, accessible at:*

<https://sphn.ch/document/ethical-framework/>

<https://sphn.ch/document/information-security-policy/>

The RECIPIENT agrees to immediately report (i) any actual or suspected data protection breach, including a breach against applicable data protection regulation, data protection section of this Agreement, (ii) any actual or suspected impairment or inadequacy of the RECIPIENT in fulfilling data protection section of this Agreement, and (iii) any application to receive or any actual access to data by an authority, unless such reporting is not admissible under statutory provisions for important reasons of public interest.

The RECIPIENT shall have in place procedures so that any person it authorizes to have access to the DATA, including the RECIPIENT’S PROJECT LEADER and their authorized users, will respect and maintain the confidentiality and security of the DATA. Any person acting under the authority of the RECIPIENT shall be obligated to process the DATA only on instructions from the RECIPIENT’S PROJECT LEADER.

In case the RECIPIENT’S PROJECT LEADER or the PROVIDER’S PROJECT LEADER is replaced, the other PARTY must be notified without delay. The RECIPIENT and the RECIPIENT’s authorized users shall not (i) provide any output or RESULTS of the DATA to any third party, except as expressly permitted in this Agreement; or (ii) sell, lease, sublicense, copy or provide the DATA to any third party, except as expressly permitted in this Agreement.

1. **No Re-Identification**. The RECIPIENT shall not carry out any procedures with the DATA (linking, comparison, processing) with the intention to identify the DATA SUBJECT, unless requested by a DATA SUBJECT according to section III.6. below.
2. **Confidentiality.** Without prejudice to provisions (in particular section III.6-9 below) or laws with regard to the processing of personal data, each PARTY shall treat the CONFIDENTIAL INFORMATION confidential for the duration of this Agreement, including any extension thereof, and thereafter for a period of five (5) years following termination or expiry of this Agreement. Excluded from this obligation of confidentiality shall be any CONFIDENTIAL INFORMATION of which one PARTY can reasonably demonstrate that it (a) was previously known to them, or (b) is, and/or becomes, publicly available during said five (5) year period through no fault of a PARTY, or (c) is independently and lawfully developed by one PARTY. This obligation of confidentiality shall not apply to any disclosure required by law, provided that the RECIPIENT shall notify the PROVIDER of any disclosure required by law in sufficient time so that the PROVIDER may contest such requirement, if the PROVIDER so chooses. Subject to mandatory law, upon the expiration or termination of this Agreement for whatever reason, or at the earlier request of a PARTY, the other PARTY shall, at its own costs, return or destroy all originals and copies of CONFIDENTIAL INFORMATION, or, in case of CONFIDENTIAL INFORMATION stored in electronic, magnetic or digital media, shall erase or render unreadable all materials furnished (including without limitation, working papers containing any CONFIDENTIAL INFORMATION or extracts therefrom) which contain CONFIDENTIAL INFORMATION.
3. **Personal data.** Each PARTY must process personal data under this Agreement in compliance with applicable data protection laws. Each PARTY represents and warrants that any personal data of DATA SUBJECTS required for use in the RESEARCH that are obtained, handled or used by it will be obtained, handled or used in accordance with all relevant laws and regulations (and where applicable, ethical guidelines) regarding their collection, use, and subsequent disposal and that any ethics committee approvals and, as the case may be, informed DATA SUBJECTS consents required for performing the RESEARCH will be obtained prior to the use in the RESEARCH.

*Section III 6.-8. needs to be adapted respectively deleted, if anonymous data (within the meaning of applicable law) is used.*

1. **Rights of the DATA SUBJECT.** The PROVIDER shall secure the exercise of the DATA SUBJECT’s rights, including access rights, the right to rectification and erasure, and the right to object. The PARTIES shall respond to requests from the DATA SUBJECT within one month after having received the notification. Moreover, the PARTIES will provide any DATA SUBJECT with a copy or the content of this Agreement upon their request or if required by law. In case of a production request by a DATA SUBJECT, either PARTY may summarize any part of this Agreement (including its Annexes) to the extent necessary for confidentiality and data protection reasons. Finally, any DATA SUBJECT may raise damages and other claims pursuant to the applicable law relating to the transfer and/or processing of their DATA under this Agreement against either PARTY.

*Note that those data subject rights are provided both by Swiss law and the GDPR.*

1. **Revocation of Consent**. In case of DATA SUBJECT’s total or partial revocation of consent, the PROVIDER must inform the RECIPIENT of this revocation without delay depending on the consent signed by the DATA SUBJECT and must provide the pseudo-identifier of the DATA SUBJECT that revoked access to his/her DATA. In such case, if applicable, the RECIPIENT shall comply with PROVIDER’s requests to anonymize their DATA according to the HRO, unless one of the exceptions listed in Article 10 of the HRO applies. A written notification shall be sent to the PROVIDER upon receipt and after completion of the request.
2. **DATA Storage and Processing**. The DATA should not be kept by the RECIPIENT longer than necessary for the purpose of the RESEARCH, and the DATA processing must be limited to the purpose pursued, provided that the DATA SUBJECT does not decide otherwise.

**IV**. **Information about RESULTS and Publication**

1. **Information about RESULTS**. Upon the PROVIDER’s request, the RECIPIENT’S PROJECT LEADER shall keep the PROVIDER informed of the RESULTS. In case clinical actionable findings are identified according to good practice RECIPIENT’S PROJECT LEADER shall inform the PROVIDER.
2. **Publication**.

The RECIPIENT shall refrain from publishing the RESULTS until the earlier of i) publication by the PROVIDER of the results of the RESARCH in which DATA was gained or ii) \_\_\_\_\_\_\_\_\_\_[date].

*Use this part (IV.2. and 3.) in case of unpublished data (e.g. ongoing clinical study), when the PROVIDERS wants to secure that their research results can be published first. Note: these aspects can also be addressed in a separate research consortium or collaboration agreement. If this relates to an already existing agreement, make sure there is no conflict.*

1. Thereafter, the RECIPIENT shall be free to publish and disclose the RESULTS but agrees to submit the proposed disclosure to the PROVIDER for review at least thirty (30) days prior to the scheduled submission for publication or disclosure. If the PROVIDER believes that the publication or disclosure contains CONFIDENTIAL INFORMATION of the PROVIDER, the PROVIDER has the right, within a maximum of a further one (1) month from the time of receipt, to request that any such CONFIDENTIAL INFORMATION be removed from the publication or disclosure. The PROVIDER also has the right to provide comments on the manuscript and both PARTIES shall discuss in good faith to incorporate such comments into the publication or disclosure. Failure to respond within the above mentioned thirty (30) day period is considered as approval of the publication by the PROVIDER.
2. **Authorship Guidelines**. All publications of the RESULTS must be compliant with the Authorship Guidelines of the Swiss Academies of Arts and Sciences, as updated from time to time, accessible at:

<https://api.swiss-academies.ch/site/assets/files/4413/akademien_autorschaft_en.pdf>

1. **Acknowledgements**. The RECIPIENT agrees to acknowledge the PROVIDER as the source of the DATA in all written publications, posters or oral presentations.

**V. INTELLECTUAL PROPERTY RIGHTS**

1. **BACKGROUND IP**. The PARTIES agree that each PARTY shall retain all title, right and interest in and to its respective INTELLECTUAL PROPERTY RIGHTS, as of the date of entry into force of this Agreement (the “BACKGROUND IP”). Unless otherwise agreed herein, nothing in this Agreement shall be construed as a transfer, license, and/or assignment by a PARTY to the other PARTY of ownership of, title, right or interest in and to its respective BACKGROUND IP.

*Choose the appropriate regulation regarding the foreground IP.*

*Background IP means all INTELLECTUAL PROPERTY RIGHTS owned by or licensed to a Party at the start of the Project. Foreground IP means all INTELLECTUAL PROPERTY RIGHTS made in the performance of work under this agreement.*

1. ***Alternative 1:*** *The RECIPIENT is the owner of the RESULTS.*

**FOREGROUND IP.** All right, INTELLECTUAL PROPERTY RIGHTS, title and interest in and to the RESULTS (the “FOREGROUND IP”), shall be owned and vest in the RECIPIENT.

***Alternative 2:*** *The RECIPIENT only is the owner of the Result but the PROVIDER is granted a license on the Result and/or receives a portion of the revenues from the commercialization.*

**FOREGROUND IP.** All right, INTELLECTUAL PROPERTY RIGHTS, title and interest in and to the RESULTS (the “FOREGROUND IP”), shall be owned and vest in the RECIPIENT.

**License on FOREGROUND IP.** RECIPIENT hereby grants to PROVIDER a royalty-free, worldwide, non-transferrable, non-exclusive, irrevocable license to access and use the FOREGROUND IP for purpose of internal scientific RESEARCH only.

and*/or*

**Royalties.** RECIPIENT will pay to PROVIDER [a fair share of *or* [...]% on] any net revenues received by RECIPIENT for the commercialization of the FOREGROUND IP.

***Alternative 3:*** *The IP is jointly owned by the PARTIES.*

**FOREGROUND IP.** All right, INTELLECTUAL PROPERTY RIGHTS, title and interest in and to the RESULTS shall be owned jointly by the PARTIES (the “JOINT FOREGROUND IP”). The PARTIES will set forth, by separate mutual agreement, their respective rights, duties and responsibility relating to the JOINT FOREGROUND IP. Such an agreement shall not cause a delay of publication of the RESULTS any longer than as defined in Section IV.2.

**VI. Compliance**

1. **Compliance with Law**. Each PARTY undertakes to comply at all time with all applicable Swiss laws, applicable international statutes, regulations and guidelines, especially all laws, statutes and regulations concerning human research and personal data protection, including any necessary regulatory approvals.

**VII. Expiration and Termination**

1. **Expiration**. Subject to the approval of the appropriate ethics committee(s) if any, this Agreement shall become effective on the EFFECTIVE DATE, and it shall automatically expire at the completion of the RESEARCH (according to the research plan as described in **Annex II**) or at the termination of the RESEARCH for any reason.
2. **Termination**. Each PARTY may terminate this Agreement at any time by giving a three months prior written notice, unless a material breach of this Agreement by the other PARTY occurs. In such case, the PARTY that suffers the material breach may terminate this Agreement by written notice to the other PARTY, which is either incapable of remedy or has not been remedied within 30 days’ notice from such breach. If the breach has not been rectified within said period, the other PARTY can terminate the breaching PARTY’s participation with immediate effect and all rights granted to the breaching PARTY according to this Agreement, will cease immediately upon receipt of the formal termination notice. If the breaching PARTY is the PROVIDER, the PROVIDER shall continue to grant access to its DATA as if it had remained a PARTY for the whole duration of the PROJECT. However, it shall have no rights whatsoever to the RESULTS subsequently generated by the RECIPIENT after effective termination.

*Adapt the appropriate time-limit if needed.*

1. **Survival Clauses**. The provisions concerning CONFIDENTIAL INFORMATION, publications, INTELLECTUAL PROPERTY RIGHTS, warranty and liability as well as those intended to protect the rights of participants / DATA SUBJECTS shall survive the Agreement’s expiration.

**VIII. Liability and Third-Party Rights**

1. **Liability**. Each PARTY shall be liable to the other PARTY for actual costs, charges, damages, expenses or losses suffered by the other PARTY resulting from any of the first PARTY’s violation of this Agreement.
2. **DATA SUBJECT’S Rights**. The PARTIES agree that a DATA SUBJECT shall have the right to enforce, as a third-party beneficiary, this Agreement against the RECIPIENT or the PROVIDER, for their respective breach of their contractual obligations, with regard to their DATA. In cases involving allegations of breach by the RECIPIENT, the PARTIES agree that the PROVIDER may take appropriate action to enforce their rights against the RECIPIENT. A DATA SUBJECT is entitled to proceed directly against the PROVIDER that has failed to use reasonable efforts to determine that the RECIPIENT is able to satisfy its legal obligations under this Agreement (the PROVIDER shall have the burden to prove that it took reasonable efforts).
3. **FOREGROUND IP**. The PARTIES use the FOREGROUND IP at their own risk. A PARTY using any of the FOREGROUND IP shall, to the fullest extent permitted by the applicable law, defend, indemnify and hold the other PARTY harmless against third party claims (including but not limited to claims based on mandatory product liability law) which are based on the PARTY’s use of the FOREGROUND IP.

**IX. General Provisions**

1. **Entire Agreement.** This Agreement represents this entire Agreement among the PARTIES with respect to the subject matter hereof, and may only be altered or amended by an instrument in writing signed by all of the PARTIES.
2. **Severability and No Waiver**. If any portion of this Agreement is in violation of any applicable regulation, or is unenforceable or void for any reason whatsoever, it should be put in writing and discussed by the PARTIES. Such portion will be inoperative and the remainder of this Agreement will be binding upon the PARTIES.
3. **Counterparts and Electronic Form.** This Agreement may be executed in any number of counterparts, each of which shall be deemed an original and all of which shall together be deemed to constitute one and the same Agreement. Each Party acknowledges that an original signature or a copy thereof, including a “portable document format” or PDF copy, or a signature generated by industry standard electronic signature software (e.g. Docusign), which is transmitted by email shall constitute an original signature for purposes of this Agreement and shall have the same legal force and effect as the exchange of original signatures; while the term “in writing” shall include communications by email or other electronic forms.
4. **Governing Law and Jurisdiction**. This Agreement will be construed, governed, interpreted and enforced according to the laws of Switzerland. All disputes arising out of or in relation to this Agreement will be brought before the competent court at the seat of the defending PARTY. In case of disputes, the PARTIES will consult each other before taking any legal action.
5. **Contact Point:** The RECIPIENT’S PROJECT LEADER is the contact point within its organization, authorized to respond to enquiries concerning this Agreement, and will cooperate in good faith with the PROVIDER within a reasonable time.

**X. Annexes**

**Annex I:** Transfer and Access Rules for Data and Meta Data

**Annex II:** Research Project

**Annex III:** Minimal Security Requirement

**IN WITNESS WHEREOF**, the PARTIES have executed this Agreement, in duplicate originals, as of the EFFECTIVE DATE.

*Add all responsible project leaders per institution/hospital and, if applicable, the duly authorized representative of the institution/hospital. The duly authorized representative is a person who is entitled to sign the institutional data sharing in accordance with signatures rules of the institution (e.g. director of research department, member of the institution’s executive board). Add an additional signature line, if you need for example to add the CEO.*

*To facilitate and accelerate the signature process, add one new page (separate page) per institution/hospital.*

*Note that the electronic unqualified signatures (e.g. using Docusign) might be allowed, but, depending on the institutional process, a wet ink signature on paper might be required. Please contact your legal department to clarify the respective process, if needed.*

**[PARTY’S NAME]**

**Project Leader Duly Authorized Representative**

[Name] [Name]

[Title] [Title]

**IN WITNESS WHEREOF**, the PARTIES have executed this Agreement, in duplicate originals, as of the EFFECTIVE DATE.

**[PARTY’S NAME]**

**Project Leader Duly Authorized Representative**

[Name] [Name]

[Title] [Title]

**ANNEX I: TRANSFER AND ACCESS RULES FOR DATA AND META DATA**

The following DATA and meta data shall be provided from PROVIDER to RECIPIENT:

[•]

*Specify the data used in the project and the applicable transfer process, e.g.*

*The XX registry, built by 4 University Hospitals, will comprise digital information about*

* *clinical data*
* *laboratory variables*
* *drugs*
* *electrocardiograms*
* *imaging data (TTEs, MRIs)*
* *outcomes*

*Number of patients/site:*

*Duration of project:*

The following access rules to DATA and meta data shall apply for PROVIDER and RECIPIENT:

[•]

*Specify who of the parties has access to the data and who is responsible to give access to the data.*

**ANNEX II: RESEARCH PROJECT**

The RESEARCH shall be limited to use of the DATA in connection with the following activities:

[•]

*Please add the research protocol and if applicable the ethics approval.*

**Annex III: Minimal Security Requirement**

RECIPIENT shall at least maintain technical and organisational measures that guarantee the confidentiality, integrity, availability and resilience of the systems with regard to processing of data. In particular, the RECIPIENT must:

* deny unauthorized persons access to facilities and data processing systems;
* ensure that unauthorised persons are prevented from reading, copying, altering or deleting data in/from data processing systems;
* ensure that unauthorized persons are not able to read, copy, modify or remove data upon the electronic transfer of data as well as during the transport of data carriers or saving of data thereon;
* ensure that it is possible to examine and verify if, when and by whom data was entered into the data processing system;
* ensure that data is protected from accidental destruction or loss;
* ensure that data received is not combined with other data unless explicitly authorized by the competent ethics commission for the specific research project and necessary to conduct the specific research project;
* restrict the disclosure and handling of data to those persons who require it to conduct the specified research project and to be able to identify each of them;
* ensure adequate organisational measures to protect data, especially by selecting, instructing and supervising employees involved in the processing of data diligently and appropriately, by guaranteeing the availability of: adequate confidentiality and data protection guidelines, regular data protection and privacy trainings, documentation of all organisational measures;
* ensure that the effectiveness of technical and organisational measures is regularly reviewed and assessed;
* implement corrective measures and immediate reporting in case of any suspected data security breach.

Make sure the minimal security requirements are met or adapt accordingly.