**DATA TRANSFER AND PROCESSING 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 | 20.11.2021 |  | DTUA V2.0 with included DTPA; 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;VII.20 ‘Counterparts and Electronic form’ wording adapted, IV.12.3 Regional node’s policies changed; V.15.1 Liability wording changed; links updated | JM |

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

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

for the [name of the project] project

*The data “Provider” (e.g. a hospital) and the data “Recipient” (e.g. a university) jointly determine the purpose and means of the processing within the framework of the research project. They both assume the role of "Data Controller". 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.*

Dated: [Date]

between

name], [address]

and

[name], [address]

(the “**PROVIDER**” and “**RECIPIENT**”, together the“**PRINCIPALS**”)

and

**SIB Swiss Institute of Bioinformatics** (Core-IT), the Romandie BioMedIT Node, with a business address at Quartier Sorge - Bâtiment Amphipôle, 1015 Lausanne, Switzerland

[and / or]

**University of Basel** (sciCORE), the Basel BioMedIT Node, Petersplatz 1, Postfach, 4001 Basel, Switzerland.

[and / or]

**ETH Zürich**, with (SIS ETHZ) being the Zurich BioMedIT Node, Rämistrasse 101, 8092 Zürich, Switzerland

(each a **Regional** **Node** and together the **BioMedIT Nodes**)

*Add all parties involved:*

* *The institutions that are providing data for the project (e.g. University Hospital Basel (USB), Spitalstrasse 21 / Petersgraben 4, CH - 4031 Basel) to the processor as well as the data recipients.*
* *The institutions hosting the BioMedIT node as a processor and providing project related services, as specified in the Appendix 1. Choose the respective nodes relevant for the project. Note that at least two nodes have to be chosen, since this template is created for multiple nodes.*

(Provider and the BioMedIT Nodes, the **Parties**)

PREAMBLE

1. Provider is the controller of data, as set forth in **Appendix 1** of this Agreement.
2. The BioMedIT Nodes form together a coordinated Swiss nationwide network of secured IT network, consisting of high performance compute and storage infrastructure, in order to support computational biomedical research and clinical bioinformatics. For the sake of clarity, and subject to the provisions of this Agreement, the Regional Nodes are independent legal entities and act as independent contractors.
3. Through the BioMedIT Network, the BioMedIT Nodes enable inter alia Swiss national or international data providers, to transfer their clinical or other data to selected researchers and other designated recipients (each a **Recipient**).
4. The Provider wishes to benefit from the BioMedIT Nodes services as described in this Agreement to inter alia store data on the BioMedIT Network and transfer Data to Recipients.

## Definitions

* 1. Unless otherwise defined in this Agreement, terms shall have the meaning described in the SPHN Glossary

<https://sphn.ch/document/sphn-glossary/>

or in the absence thereof, as provided by applicable laws.

* 1. Capitalized terms, whether used in singular or plural form, shall have the following meaning:

**Data**: means all the data, including the clinical, laboratory and radiology data, and/or meta data, as well as any Personal Data contained therein, being transferred (or if not transferred, the data given access to) under this Agreement, as set forth in **Appendix 1** of this Agreement.

**Confidential Information**: means any data, documents, information or other material (in any form) that is identified as confidential in writing, or otherwise designated in writing as confidential, or which may reasonably be regarded as confidential, and which is disclosed hereunder by a Party to another Party.

**Data Subject**: means any data subject whose personal data are included in the Data*.*

**Intellectual Property Rights**: means all rights, title and interest, registered or not, whether arising from Swiss or any other national or international legislation, in copyright, databases, trademark, domain names, designs and patents of invention, know-how, confidentiality and/or business secrets, and all other intellectual property or similar proprietary rights of whatever nature.

**Principals**: means the Provider and the Recipients jointly.

## General Terms of Services

1. Services
   1. In General. Subject to, and in accordance with, the terms of this Agreement, each Regional Node undertake to provide to Provider the services specified in Section II.2.2 (the **Services**) to the best of its ability using all reasonable skill and care, and always subject to Provider’s compliance with all its obligations under the Agreement.
   2. Scope. The Services consist of, except as otherwise specified in **Appendix 1**, the following:
      1. hosting of the Data on the BioMedIT Nodes;
      2. transferring Data to Recipients in accordance with this Agreement; and
      3. other processing activities as required under this Agreement or as reasonably requested by Provider.
   3. Collaboration with and between Regional Nodes. Services are provided by the Regional Nodes as described in **Appendix 1**. The Parties shall specify **in Appendix 1** which Regional Node shall be primarily responsible for providing the Services. Each Regional Node undertakes to collaborate with the other Regional Nodes, and to assist them, as may be required for the proper providing of the Services.
2. Financial Terms
   1. Payment of Fees. Costs associated to the Services to be provided by Regional Nodes shall be determined by mutual agreement between the Parties once the project for which Provider needs the BioMedIT Network has been validated by the competent ethics committee.

[Or]

Payment of Fees. The Services are part of the SPHN initiative and are provided without any associated costs, unless it surpassed a specifically defined upper limit of compute, storage or human resources.

Choose or adapt the appropriate payment regulation.

1. Main Point of Contact
   1. Designation. Provider shall designate in **Appendix 1** one or several persons within its organization to act as main point of contact (each a **MPOC**). Provider may from time to time, by means of a written notice to all BioMedIT Nodes, remove, change or add any MPOC, provided that there shall always be at least one MPOC.
   2. Power. Each MPOC shall have the individual power to give instructions to, and receive notification from, the BioMedIT Nodes, on behalf of the Provider, for all actions relating to the Data, including for the purpose of Section II.5. below.
2. Transfers to Recipients
   1. In General. Provider may, by an instruction through a MPOC, designate selected Recipients to which all or part of the Data shall be transferred to.
   2. Means of Transfer. Except as otherwise agreed in writing, Data shall be transferred by providing to Recipients remote secured access to the Data in accordance with the security standards specified in Section III.8.1. The BioMedIT Nodes and the Provider shall decide on a case by case basis from which Regional Node the Data shall be made available.
   3. Responsibility. Provider shall ensure that the Recipients:
      1. comply with the security requirement of Section III.8.1 and have in place procedures so that any person to which access to Data is being granted maintain the confidentiality and security of the Data;
      2. maintain the confidentiality of any credential and/or passwords required to access the Data and immediately inform the relevant Regional Node of any loss or unauthorized disclosure of such credential and/or passwords, or if any authorised user for whom credentials have been issued quits Recipient’s organization. The BioMedIT Nodes shall neither be responsible in case of improper use of the said credentials by Recipients nor in case of access and / or use by an unauthorized third party.

## Data Processing Terms

1. Supply of Data

# Provider shall provide the Data to the selected Regional Node, or make the Data available to it, in the form and as specified in **Appendix 1**.

1. Scope of Processing
   1. In General. The Parties acknowledge and agree that:
      1. the subject matter and details of the processing are specified in this Agreement and its **Appendix 1**;
      2. the BioMedIT Nodes are joint processors of the Data;
      3. Provider is a Controller of the Data;
      4. any Recipient to which Data is transferred under this Agreement shall be deemed Controller;
      5. each Party shall comply with its obligations under any applicable laws with regard to the processing of the Data (including data protection laws, as well as laws, statutes and regulations concerning human research and personal data protection).
   2. Nature and Purpose of Processing. The BioMedIT Nodes shall process the Data on behalf of the Principals and solely for the purpose of providing the Services or as otherwise expressly instructed by a MPOC or agreed with Provider. For the sake of clarity, the BioMedIT Nodes shall have no obligation to carry out any instruction which they consider, at their sole discretion, to be unlawful, ambiguous, doubtful or unclear (in which case the Parties shall collaborate in good faith to find a solution agreeable to all).
   3. Restrictions. The BioMedIT Nodes shall not, without the prior written consent of Provider:
      1. subcontract any of their processing operations of the Data (except to another Regional Node); and
      2. transfer the Data in any country outside Switzerland (it being agreed that the Data may be accessed and processed by Principals outside Switzerland, in which case Provider shall be responsible for compliance with any applicable data protection obligation).
   4. Return of Data. Upon termination of the Agreement, or earlier as requested by Provider, the BioMedIT Nodes shall, within reasonable time following a written request by Provider, provide Provider with a final extract of the Data and permanently delete all copies of such Data still under its control. In any case, the BioMedIT Nodes shall be allowed to permanently delete the Data 60 days after termination of the Agreement.
2. Security
   1. Security Requirements. Each Party processing Data shall do so 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’). Data processing shall comply with the “*Ethical Framework for Responsible Data Processing in Personalized Health Research*” and with 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 BioMedIT Nodes shall comply with the Minimal Security Requirements provided for in **Appendix 3**.

* 1. Security compliance. Each Party shall take appropriate measures to ensure compliance with the above-mentioned security measures by its employees and subcontractors, in particular by ensuring that all persons authorised to handle Data are committed to maintain confidentiality or are subject to an appropriate legal obligation of confidentiality.

Security Incidents. Each Regional Node agrees to immediately report, by any useful means (in particular via the MPOC), (i) any actual or suspected data protection breach, including a breach against applicable data protection regulation, data protection section of this Agreement, or any accidental or unauthorized access to the Data (ii) any actual or suspected impairment or inadequacy of the BioMedIT Node 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.

In case of accidental or unauthorized access to the Data, the Regional Node shall, to the extent possible, describe the nature of the security incident, as well as any measures taken by it to mitigate potential risks and the measures that it recommends Provider and/or Recipient to take. Provider shall be responsible for complying with the legal provisions applicable to it, in particular any obligations of Provider to provide a notification of the incident to any competent authority and/or the Data Subjects. In this context, the Regional Node shall provide Provider with any assistance reasonably required by Provider in order to comply with its obligations.

1. Representations and Warranties

Provider represents and warrants that:

* + 1. the Data has been collected, transferred and processed in accordance with the requirements of all applicable laws, rules and regulations, including all applicable data protection laws and regulations;
    2. the transfer to the BioMedIT Nodes and the processing of the Data by the BioMedIT Nodes (including any further transfer to Recipients) as set forth in this Agreement is (i) admissible under all applicable laws, rules and regulations and (ii) is not prohibited by a statutory or contractual duty of confidentiality;
    3. prior to any collection, transfer, and processing of personal data contained in the Data, Provider has provided to the concerned Data Subjects all required information (including in relation to any processing activity contemplated under this Agreement) and has complied with any notification and registration obligations under any applicable laws and regulations;
    4. Provider will not require the BioMedIT Nodes to undertake a processing of Data that Provider would not be permitted to carry out itself.
    5. Provider has and will verify that the technical and organizational measures, as required by all applicable laws, rules and regulations, undertaken by the BioMedIT Nodes, in particular with the Appendix 3, the “Ethical Framework for Responsible Data Processing in SPHN” and the “SPHN Information Security Policy” (see Section III.8.1), are sufficient to protect the Data from any unauthorized processing. Provider warrants that the technical and organizational measures set forth in Section III.8.1 are sufficient in this regard.

1. Information, Assistance and Notifications
   1. Compliance. Each Party shall provide the other Parties with all the necessary information so that they can demonstrate compliance with their obligations under the applicable data protection legislation.
   2. Requests from data subjects. Provider shall be responsible for the handling of any Data Subject request and to provide Data Subjects with their right in accordance with data protection laws. If a Regional Node receives a request from a Data Subject, it shall direct the Data Subject to submit its request to Provider and shall assist Provider in the handling of such request, as may be reasonably required.
   3. Impact assessments and prior consultation. The BioMedIT Nodes undertake, to the extent they can reasonably be expected to do so in light of the nature of the processing and the information available to them, to assist the Principals in ensuring their compliance with their impact assessment, prior consultation and records of processing activities obligations (if any).
   4. Notification and assistance. Each Regional Node processing Data shall promptly inform, and cooperate with, Provider if it considers that it may no longer be able, or is no longer able, to comply with this Agreement, particularly in case it receives or must reasonably expect to receive a request or order of a competent authority requiring it to disclose, or refrain from further processing, some or all personal Data to which this Agreement applies.
   5. Audits. The provisions of **Appendix 2** shall apply regarding audits.
2. Register of Processing Activities
   1. Provider acknowledges that the BioMedIT Nodes may be required by the law to:
      1. collect and store certain information, including the name and contact details of each processor and/or controller with whom the BioMedIT Nodes act and, where applicable, the local representative of the controller and/or the data protection officer as well as the categories of processing carried out; and
      2. make such information available to any competent authority.
   2. Provider undertakes to provide the BioMedIT Nodes with all information reasonably necessary for the BioMedIT Nodes to meet their obligations.

## Data ownership, Intellectual Property, Confidentiality

1. Data Ownership and Right to Use
   1. Ownership. As between Provider and the BioMedIT Nodes, Data is and shall remain the sole and exclusive property of Provider and all right, title, and interest in the same (including any Intellectual Property Right) is reserved by Provider. Subject to Section IV. 12.2, nothing in this Agreement is intended to assign or grant the BioMedIT Nodes any Intellectual Property Rights or other rights in the Data.
   2. Use of Data. Provider grants to the BioMedIT Nodes a right to access and use the Data for the sole purpose of, and only to the extent necessary for, providing the Services, including a license to collect, process, store, generate, and display the Data.
   3. Regional Node’s Policies. Principals undertake to comply with the Acceptable Use Policy and other internal policies (e.g., service level agreement) specific to each Regional Node. Provider also undertakes, within the framework of its agreements with the Recipient, to require the Recipient to comply with such regulations.
2. Confidentiality
   1. In General. Without prejudice to special provisions 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.
   2. Required disclosures. This obligation of confidentiality shall not apply to any disclosure required by law, provided that the Party subject to the disclosure obligation shall notify the concerned Parties of any disclosure required by law in sufficient time so that they may contest such requirement, if they so choose.
   3. Return. Subject to mandatory law, upon the expiration or termination of this Agreement for whatever reason, or at the earlier request of a the concerned Party, the other Parties to which Confidential Information have been disclosed shall, at their 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. IP in BioMedIT Nodes

# As between Provider and the BioMedIT Nodes, the BioMedIT Nodes shall be and remain the sole owner of all Intellectual Property Rights in and to the BioMedIT Nodes, as well as any other infrastructure used to provide the Services. Nothing in this Agreement is intended to assign or grant Provider or any other Principal any Intellectual Property Rights or other rights of the BioMedIT Nodes.

## Liability

1. Liability
   1. The Parties agree to each be solely responsible for all acts or omissions in the performance of their respective duties hereunder, and shall be financially and legally responsible for all liabilities, costs, damages, expenses and attorney fees resulting from, or attributable to any and all such acts or omissions.
   2. Each Party disclaims any liability for any indirect damages or losses, whether foreseen or foreseeable, related to the loss of use, interruption of business, loss of actual or anticipated profit, loss of revenue, loss of anticipated savings, loss of opportunity, loss of goodwill, loss of reputation, loss of, damage to or corruption of assets or data, or any other indirect, incidental, exemplary, or consequential damages or losses of any kind, regardless of the form of action, whether in contract, tort or otherwise.

## Term

1. Term

This DTPA shall become effective on the date when it is signed by the duly authorized representatives of one BIOMEDIT NODE, and then for each additional BIOMEDIT NODE, on the date when the duly authorized representatives of each additional BIOMEDIT NODE adhere and sign this DTPA.

1. Termination
   1. Termination for Convenience. Each Party may terminate the Agreement for any reason at any time upon 3 months prior written notice to the other Parties. A termination by a Party shall have the effect of terminating the Agreement for all Parties, except as otherwise agreed in writing by the non-terminating Parties.
   2. Termination for Cause. Each Party may terminate the Agreement with immediate effect, if another Party has materially breached or is in material breach of its obligations and such breach is not cured, or the breaching Party is not diligently pursuing a cure, within 30 days after written notice of breach.
2. Survival

# All terms which are expressed or intended to survive, and any provisions of the Agreement necessary for its interpretation or enforcement will continue to apply regardless of the reason for termination of the Agreement.

## Miscellaneous

1. Independent Contractors

Nothing in the Agreement is intended to, or shall be deemed to, establish any partnership or joint venture between the Parties, constitute any Party the agent of the other Party, nor authorise any Party to make or enter into any commitments for or on behalf of the other Party. Neither Party shall have the power to incur any obligations in the name of, or on behalf of, or pledge credit of, the other Party in any manner whatsoever.

1. 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.

1. Assignment

# No Party may transfer this Agreement, or assign in whole or in part its rights or obligations under this Agreement, without the prior written consent of the other Parties. Any transfer or assignment made without such consent shall be null.

1. Force Majeure

# No Party shall be considered in default under this Agreement if all or any of its obligations (other than for payment obligations) are delayed or prevented as a result of a situation of force majeure, such as natural disasters of a particular intensity, war, riot, strike, power failure or Internet network failure, or any other cause that is reasonably beyond the control of the affected Party.

1. Amendment

# This Agreement (including this section) may be amended only by a written instrument duly signed by the Parties.

1. Entire Agreement and Hierarchy
   1. This Agreement, together with its appendices and the future agreement regarding the Payment of Fees according to article 3.1, constitutes the entire agreement between the Parties with respect to its subject matter and supersedes all prior agreements between the Parties with respect to its subject matter.
   2. In the event of conflict with an appendix to this Agreement, this main body of this Agreement will govern, unless the appendix specifically states its intent to do so and cites the section or sections amended.
2. Severability

# If any provision of this Agreement is held to be invalid or unenforceable for any reason, the Parties shall replace it by a substitute provision that achieves to the fullest extent possible the same legal and economic purposes as those of the invalid or unenforceable provision. In any event, the remainder of this Agreement shall remain in full force and effect between the Parties.

1. No Waiver

# The failure of any of the Parties to enforce any of the provisions of this Agreement or any rights with respect thereto shall in no way be considered as a waiver of such provisions or rights or in any way affect the validity of this Agreement. The waiver of any breach of this Agreement by any Party shall not be construed as a waiver of any other prior or subsequent breach.

## Governing Law and Jurisdiction

1. Governing Law

# This Agreement shall be governed by and construed in accordance with Swiss substantive law, without reference to its conflict of law provisions.

1. Jurisdiction

# Any dispute or difference arising out of or in relation to this Agreement shall be subject to the exclusive jurisdiction of Swiss courts at the registered seat of the defending Party, subject to the right of appeal to the Federal Tribunal.

[*signature page follows*]

|  |  |
| --- | --- |
| **Principals**  **[name]**, [address] | |
| [Name]  [Title]  Date: | [Name]  [Title]  Date: |
| **Principals**  **[name]**, [address] | |
| [Name]  [Title]  Date: | [Name]  [Title]  Date: |
| **BioMedIT Nodes**  **SIB Swiss Institute of Bioinformatics** (Core-IT, Romandie BioMed-IT Node) | |
| Ron Appel  SIB Executive Director  Date: | Heinz Stockinger  Head of Core-IT  Date: |
| **[**and/or**]**,  **University of Basel** (sciCORE, Basel BioMed-IT Node) | |
| Torsten Schwede  Vice President for Research, University of Basel Date: | Thierry Sengstag  Associate director – sciCORE, Center for Scientific Computing  Date: |
| **[**and/or**]**,  **ETH Zürich** (SIS, ETHZ BioMedIT Node) | |
| Bernd Rinn  Head of SIS  Date:  *Choose the respective nodes.* | Rui Brandao  Head of IT-Services  Date: |

**Appendix 1 to the DTPA – Description of Data and Service**

*This Exhibit 1 should in particular include the information provided for in Sections I./1.2, II./2.2-3, II./4.1 and III./6 of the DTPA.*

1. **Description and format of DATA**

*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:*

1. **Supply of Data to the BioMedIT Nodes**

[●]

# Transfer of Data

Data will be transferred to the BioMedIT Nodes within a standardized and secure way, i.e. using the network-internal Data Transfer Tool. Data is stored and processed in compliance with the SPHN Information Security Policy.

Adapt the information given for the transfer of data, if needed.

# Data access

The Project Lead [ ] defines who will be authorized to access the Data. Only authorized users can access and process the data. Login to the secure BioMedIT Node requires two-factor authentication and access to data is only possible via trusted networks (either from within Swiss university and university hospital networks or via VPN). For this project access will be provided to [ ]. Access to the Internet is strictly controlled, limited to trusted and explicitly whitelisted web resources. Contractual and technical measures prevent that data is shared and/or combined without the appropriate authorization. Transfer, access and processing operations are logged. Physical access to server rooms of BioMedIT nodes is access-controlled.

Specify who defines the access rules and who has explicitly access to the data.

1. **Services**

As specified in the Agreement.

All three BIOMEDIT NODES provide services to the PROVIDER.

Specifically:

* [ ] is the main BIOMEDIT NODE for this project. It is providing the processing services mandated by the PROVIDER to fulfill the project goals, including data storage (hosting), computational resources for data analyses, transfer of data, etc.,
* [ ] will provide services related to transfer of data,
* [ ] will provide services related to transfer of data.

Specify who acts as main node and provide additional services, if applicable.

**D. Main Project Leader respectively MPOC**

[Name, address, email]

**Appendix 2 – Information And Audits of Security Measures**

1. Scope. The provisions of this Schedule apply to personal data contained in the Data.
2. Information The BioMedIT Nodes shall make available to Provider, all documents and information reasonably necessary to demonstrate their respective compliance with the applicable data protection law and their obligations arising therefrom.
3. Right of audit. The BioMedIT Nodes shall allow Provider or an independent auditor appointed by Provider to conduct audits (including inspections) to verify the BioMedIT Nodes' compliance with their obligations under the applicable data protection law. Any audit shall be constrained to infrastructure needed to perform this Agreement/ Project and related measures. The BioMedIT Nodes shall provide reasonable assistance with respect to the audits described in this clause 3. Upon conclusion of the audit, Provider shall forward the complete audit report to the BioMedIT Nodes, free of charge.
4. Request. Any request under clause 2 (Information) or clause 3 (Audits) must be communicated to the BioMedIT Nodes in writing and indicate (i) the Data concerned, (ii) the reasons for which the conditions referred to in clause 2 (Information), respectively clause 3 (Audits) apply to these Data, (iii) the specific documents to be reviewed, respectively the specific obligations of the BioMedIT Nodes to be audited, and (iv) that Provider expressly undertakes to use the information collected only to ensure that the BioMedIT Nodes are in compliance with their obligations with regard to the concerned Data. Unless there are exceptional circumstances, Provider may not make more than one request per year.
5. Exercise of rights. Upon receiving a request in accordance with the preceding clause, and provided that all conditions are met, the BioMedIT Nodes shall comply with the request as follows:
6. the BioMedIT Nodes shall inform Provider, with regard to the review of documents (clause 2 [Information] above), of the period during which it may consult the documents at the BioMedIT Node's offices. Unless otherwise expressly agreed by the BioMedIT Nodes, Provider shall not be authorised to make copies of the documents consulted. Alternatively, the BioMedIT Nodes may decide to provide the documents electronically;
7. the BioMedIT Nodes shall inform Provider with regard to audits (clause 3 [Audit] above) of (i) the date or dates on which the audits may take place and (ii) the scope of the audit, in particular the inspections that may be carried out, in order to check the BioMedIT Nodes' compliance with their obligations under this Agreement. Provider's internal costs or the costs of the independent auditor appointed by it shall be borne entirely by Provider. The BioMedIT Nodes may invoice Provider for their own costs associated with the preparation for and execution of the audit based on the costs incurred by the BioMedIT Nodes. The BioMedIT Nodes may object to any independent auditor appointed by Provider if, in their opinion, the auditor is not sufficiently qualified, is a competitor of the BioMedIT Nodes, or in any other way would not be able to perform its duties properly. In this case, Provider may either carry out the audit itself or propose another auditor to the BioMedIT Nodes.
8. Confidential information. The provisions contained in this clause 2 shall not be interpreted as requiring the BioMedIT Nodes to provide Provider with (i) any information relating to trade secrets of the BioMedIT Nodes or any information of a confidential nature or (ii) any information concerning other users of the BioMedIT Nodes' services. The BioMedIT Nodes may make the review of documents (clause 2 [Information] above) or the conduct of an audit (clause 3 [Audits] above) subject to the conclusion of a specific confidentiality agreement.

**\* \* \* \***

**Appendix 3 – Minimal Security Requirements**

The BioMedIT Nodes shall ensure that the technical and organisational measures it provides are sufficient to guarantee the confidentiality, integrity, availability and resilience of the systems with regard to processing of data. In particular, the BioMedIT Nodes 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.