# [Fil:Region hovedstaden logo.png](http://upload.wikimedia.org/wikipedia/commons/b/bc/Region_hovedstaden_logo.png)

**Internal Service Agreement**

This Internal Service Agreement (hereinafter referred to the “Agreement”) is entered into by internal units of Region Hovedstaden, Rigshospitalet, Blegdamsvej 9, DK-2100 Copenhagen, Denmark, CVR No. 29190623 regarding:

**NEUROBIOLOGY RESEARCH UNIT**, Section 8057

Represented by: Dr Cyril Pernet, [cyril.pernet@nru.dk](mailto:cyril.pernet@nru.dk)

(Hereinafter referred to as “NRU”)

and

**DEPARTMENT OF CLINICAL PHYSIOLOGY AND NUCLEAR MEDICINE**,Section 4011

Represented by:

Contact person:

(Hereinafter referred to as “**Institution**”).

Both parties individually referred to as “Party” and jointly referred to as the “Parties”.

**WHEREAS** the Parties are internal sections within Rigshospitalet and share the same organizational affiliation and wish to collaborate on the project titled “HEDIT: Healthy Digital Twin”. Any and all

**WHEREAS**, NRU has developed a data sharing service (the Public-nEUro platform, detailed in Schedule A that facilitates sharing of brain imaging research data in accordance with the European General Data Protection Regulation (GDPR), and in compliance with the FAIR principles (i.e., that research data should be Findable, Accessible, Interoperable and Reusable);

**WHEREAS,** Institution being in possession of brain imaging research data obtained by research projects carried out at Institution on synaptic density PET with associated PET-MR data (hereinafter referred to as Institution Data) and wishes to make Institution Data available to interested users via the Public-nEUro platform;

NOW, THEREFORE, in consideration of the foregoing, the Parties have entered into this Agreement on the following terms and conditions:

# Definitions

In this Agreement the following terms shall have the meanings:

“Services” shall mean the activities to be performed by NRU under the Agreement, as specified in Schedule B.

# Engagement of NRU

## NRU shall provide the Services to Institution as outlined in the attached Schedule B.

## NRU shall provide the Services at such reasonable times as may be agreed with Institution.

## NRU shall perform all such reasonable and normal duties and functions ofthe Services in accordance with the level of expertise expected of NRU and with reasonable skill, care and diligence. NRU shall also comply with the lawful and reasonable directions of Institution.

## The Institution shall provide all data and information at its disposal or reasonably requested by NRU in order for NRU to complete the Services.

2.5 This Agreement shall not constitute an employer-employee relationship. It is the intention of each Party that NRU shall be an independent contractor and not an employee of Institution.

# Remuneration

## In consideration of NRU performing the Services for Institution as outlined in Schedule B, Institution shall pay to NRU a fee in the amount as specified in Schedule B.

# Confidentiality

## If in the course of providing the Services, NRU acquires information relating to Institution’s processes, developments, business, finances and such, this information shall be deemed to be Institutions Confidential Information.

## NRU shall keep confidential all Institution Confidential Information and shall not disclose or supply to any third party outside the Institution any of the Institution Confidential Information without the prior written consent of Institution.

## NRU shall only use Institution Confidential Information for the purposes of providing the Services.

## The obligations in Clauses 4.2 shall not apply to information or any part thereof which NRU is clearly able to demonstrate:

### was known to NRU prior to their disclosure by Institution hereunder and was not acquired from Institution; or

### was in the public domain prior to its disclosure or enters into the public domain after disclosure through no fault of NRU; or

### becomes known to NRU by action of a third party not in breach of any obligation of confidentiality to Institution;

### was independently developed, or arrived at, by NRU; or

### is required to be disclosed by law or government regulation or court order.

# Publication

5.1 Institution shall properly acknowledge NRU in all publications or presentations for the Services provided.

5.2 Institution acknowledges and accepts that NRU may use the Institution Data for quality control, meta-analyses and creation of brain imaging atlases, and that results from such activities can lead to academic publications and atlases that can be shared openly (CCBY) – see also, section 8.2.

5.3 NRU shall properly acknowledge Institution in all publications or presentations for the Institution Data.

# 6. Liability

6.1 NRU is subject to the generally applicable rules on liability in contracts as well as in torts under Danish law.

6.2. NRU shall obtain and maintain a professional liability insurance covering the services or be self-insured.

**7. Compliance with privacy and data protection laws**

7.1 The Parties acknowledge and agree that they are separately responsible for complying with applicable data protection law.

7.2 As personal data is to be processed by NRU on behalf of Institution during the performance of the Services, the Parties will enter into a Data Processing Agreement as per Schedule C, in accordance with European General Data Protection Regulation (GDPR).

7.3. Due to the internal nature of the agreement the parties acknowledge to be governed by Region Hovedstaden as data controller.

# 8. Intellectual Property

## 8.1 Any data, results, analyses, knowledge, Information and inventions derived from the Services performed by NRU under this Agreement, defined in Clause 5.3, shall be the sole property of NRU.

## 8.2 If NRU uses the Institutions data for other purposes than those defined in Clause 5.2, it will be governed by the Institution Data User Agreement

## 8.3 Notwithstanding Clause 8.1, Institution Data shall be the sole property of Institution.

# 9. Term & Termination

## This Agreement shall be effective on the date of the last signature and shall continue in force until the End Date, as specified in Schedule B unless this Agreement is terminated in accordance with Clauses 9.2 and 9.3

## Each Party may terminate this Agreement without cause at any time by giving the other party not less than 45 days’ written notice of termination.

## Notwithstanding anything to the contrary herein contained, this Agreement may be prematurely terminated on thirty (30) days written notice given by the non-breaching Party to the breaching Party should the breaching Party commit any material breach of any of its obligations under this Agreement;

## Any rights or remedies of any Party arising from any breach of this Agreement shall continue to be enforceable.

# General

## 10.1 No Party shall be entitled to assign or otherwise transfer any of its rights and/or obligations under this Agreement to any third party except with the prior written consent of the other Party.

## 10.2 No alteration, cancellation, variation of, or addition hereto shall be of any force or effect unless reduced to writing and signed by both Parties to this Agreement or their duly authorised representatives.

## 10.3 All notices given under this Agreement must be in writing and delivered to the other Party.

## 10.4 This Agreement shall be construed and interpreted pursuant to the laws of Denmark to the exclusion of any rule that would refer the subject matter to another forum. The Parties submit to exclusive jurisdiction of the competent courts of Copenhagen to resolve any dispute between them.

## **Signed for and on behalf of NRU by its duly authorised representative:**

Name: Dr Cyril Pernet

Title: Head of OpenNeuroPET, Technical Lead of Public-nEUro

Signature: A signature on a white background

AI-generated content may be incorrect.

Date

*Read and understood:*

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: Mr Peter Jensen

Title: Neurobiology Research Unit center manager

Date Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Signed for and on behalf of Institution by its duly authorised representative:**

Title:

Name:

Signature:

Date Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Read and understood:*

Name:

Title:

Date Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**SCHEDULE A - Details about Public-nEUro**

The Public-nEUro platform provides a secured infrastructure and service enabling FAIR- and GDPR-compliant sharing of Institution Data between Institution and interested users.

As depicted in the diagram below, Institution Data moves from the Institution (data controller) to NRU (data processor) who makes it available via the Public-nEUro platform. NRU processes Institution Data on behalf of Institution as defined in and controlled by the Data Processing Agreement (Schedule B), with the purpose of enabling Institution Data to be shared with registered users. Registered users must first sign the Data User Agreement (DUA) associated with the requested Institution Data, as well as a separate EU Standard Contractual Clauses if located outside the EU/EEA in a country without adequate level of data protection. The DUA sets the licensing terms between Institution (data controller) and the end users (data processor or new data controller).

A diagram of a service agreement

Description automatically generated

Institution deposits the Institution Data via a secured file transfer protocol (SFTP) to Public-nEUro. In the Public-nEUro platform, generic information describing the Institution and the Institution Datasets name and Unique ID are stored into an encrypted SQL database. Deposited data is checked for compliance, i.e., Institution Data must be in a specific format (BIDS format, see below) or be convertible to this format by NRU, and must be accompanied by an associated DUA for interested end users.

Upon successful compliance check, the Institution Data is hosted to a geographically EU constrained cloud service provider where it is stored securely and encrypted. Institution decides beforehand (Schedule B), if Institution Data released to the cloud should be privately hosted and thereby accessible to only particular users upon registration, publicly available, or openly available.

To ensure *findability* of the Institution Data for interested users, anonymized dataset metadata (a small text-based file describing the data at an aggregated group level) are made public by NRU and circulated, but not limited to, EBRAINS (the EU computational platform, <https://ebrains.eu/>), OpenNeuro (US-based repository, <https://openneuro.org/>), and CONP (Canada-based repository and computational platform, <https://portal.conp.ca/>).

*Accessibility* of the Institution Data is ensured by NRU by using a well reputed Cloud service that allows constant access to and downloading of the data for approved users. Users and users’ institutions must register and be fully identified to be given access (unless open data), which occurs on a dataset-by-dataset basis when the appropriate documents have been signed (all stored in the encrypted SQL database).

*Interoperability* and *Reusability* are ensured by accepting only brain imaging data curated in accordance with the Brain Imaging Data Structure (BIDS, https://bids.neuroimaging.io/) – an international standard to organise and name brain imaging files and add metadata describing the overall data content.

***Responsibilities of Institution:***

As the data controller, Institution ensures Institution Data were collected lawfully. Institution is responsible for providing to NRU together with deposited Institution Data an Institution DUA that is nationally lawful and compliant with the EU General Data Protection Regulation. Furthermore, Institution is responsible for the proper preparation of the deposited Institution Data. Deposited Institution Data must have been properly pseudonymized and curated into BIDS format by Institution, alternatively Institution must request NRU to perform the BIDS-data curation as part of this Agreement. In any case, Institution must remove any personal identifiers from the Institution Data before upload to Public-nEUro. Should the uploaded Institution Data contain anatomical information, Institution may, but is not required to, perform defacing of the data (i.e., to remove any facial information).

***Responsibilities of NRU:***

NRU is responsible for securely processing the deposited Institution Data and for enabling access to Institution Data by registered users who have signed the Institution’s mandatory DUA and, if needed, a separate EU Standard Contractual Clauses (EU-SCC). NRU will provide storage of the DUA and EU-SCC document templates alongside the Institution Data as well as the documents that have been signed by registered users (i.e., every access will be auditable).

When the Institution’s DUA implies transfer of data controller rights from Institution to the end user NRU will grant access to the Institution Data for a new registered user (a new Data Controller) as soon as the new user has signed the Institution’s DUA and DPIA. When relevant (as per schedule B), a separate EU-SCC for non-EU users will also be requested. This means that in this later case, Institution consents for NRU to transfer Institution Data to end users in third countries or international organisations without NRU notifying the Data Controller about it.

When, on the other hand, the Institution’s DUA only gives future users data processor rights for the Institution Data, NRU will inform the Institution immediately about new requests and will not grant access to any new user before the Institution has approved the particular request.

**SCHEDULE B – Services provided by NRU**

**Data upload to Public-nEUro and data curation:**

Upon Agreement signature, NRU will enable access for Institution to deposit Institution Data into Public-nEUro. When Institution has performed the data upload, NRU will perform the requested services, including but not limited to quality control, compliance check on all uploaded data to ensure that all datasets have been successfully pseudonymized and BIDS-curated by Institution prior to upload, metadata enhancement (e.g. metadata schemas for cross-referencing with OpenNeuro), and that they are accompanied by an associated DUA/SCC. Only identified NRU personnel have access to these data, and every login is registered. NRU does not accept Institution Dataset constituted entirely of medical records. In case Institution has requested NRU to perform the pseudonymization and BIDS-curation on their behalf (see below), Institution will instead upload raw Institution Data and then NRU will perform the needed processing steps (this does not include performing defacing, unless explicitly requested by Institution) to make all the uploaded datasets compliant and valid for further processing Public-nEUro.

**Name/Title/Reference for the Institution Data covered by the Agreement:**

Dataset\_name

**Institution will upload the following type of Data:**

Pseudonymized and BIDS-curated Institution Data,

Not-curated but pseudonymized Institution Data (hence requesting NRU to perform the BIDS-curation).

**Institution requests NRU to perform facial information removal as part of the BIDS-curation:**

**[*This question is only relevant if the “*Not-curated but pseudonymized Institution Data *“-choice has been checked above]*:**

Yes

No.

**Regarding the associated DUA and SCC to be uploaded with the Institution Data:**

Institution agrees for PublicnEUro to process DUA and SCC without Institution oversight (controller to controller SCC).

Institution requires to approve each user DUA and SCC signature before PublicnEuro gives access to the data (controller to processor SCC).

**Data access:**

When all deposited Institution Data has passed the compliance check, NRU will release the data alongside with metadata describing them, onto a cloud service that acts as NRU’s sub-processor, as defined in the Data Processing Agreement (Schedule C).

As part of the service, the Institution contact person will become a registered user of PublicNeuro and access granted by default to the Institution dataset.

Depending on the choices made by Institution below, the released Institution Data will be privately, publicly or openly hosted, and group metadata shared publicly. Public sharing means that an open public record of available data will be published and searchable on the web or other neuroimaging repository, while data access remains controlled.

**Institution agrees that the Institution Data released by NRU can be shared with:**

specific registered users from dedicated institutions (private hosting),

any registered users from institutions in EU states only (public hosting level 1),

any registered users from institutions in EU states and in counties having shown an adequate level of data protection as amended from time to time by the EU-Commission (public hosting level 2 – as of 2023: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay , The republic of Korean and the United Kingdom)

any registered users worldwide (public hosting level 3), governed by EU Standard Contractual Clauses (SCC) by utilizing Clause 7 (“Docking Clause”)

anyone worldwide (fully open, CC0 or CCBY licencing),

If required, what is your embargo duration: 0 month.

**Security measures:**

*User control: A* new user must register on Public-nEUro giving a password for future login. In conformity with best practices, any new access will also require a One-Time Password generated by a third party thus minimizing risks of giving access to an unidentified third person. All new user registrations will be manually handled by a member of the Public-nEUro team, who will ensure that the provided user information is valid. First upon manual approval of the new user, the new user will have a valid status and get access to Public-nEUro. This status will automatically be revoked after one year without activity but can be reactivated on demand (after checking the user is still at the same institution for instance). Finally, before downloading a dataset, each user must sign the Institution’s DUA and a separate EU-SCC for non-EU researchers.

*Registration and DUA:* A general possible risk associated with sharing pseudonymized data is re-identification. Since users interested in the released Institution Data are requested to register with Public-nEUro and to sign the DUA associated with the Institution Data, the DUA must state that users are not allowed to attempt to re-identify participants. The risk of re-identification and of potential harm is low since a high level of expertise is required to analyse and interpret biomedical and imaging datasets. Institution has the responsibility for the DUA being lawful, while NRU has the responsibility of not enabling access to data before the DUA has been signed. Upon request from Institution, NRU can revoke access to Public-nEUro for specific users.

*Storage and access:* All datasets (privately, publicly or openly hosted) are securely stored using NRU’s sub-contractor, Computerome (<https://www.computerome.dk/>), the Danish National life science supercomputing center. Computerome has secured read/write access, encryption in transit and geo-redundant back-ups. It meets all the compliance requirements including GDPR (EU) for health data storage (see <https://www.computerome.dk/security>), is ISAE-3000 certified and follow ISO27001.

**Creating aggregated data:**

Institution agrees that, except in the case of private hosting, NRU is allowed to process the Institution Data on their own behalf for atlasing purposes, i.e., the activity of analysing aggregated Institution Datasets in order to create reference images (section 5.2). Institution Data transferred to Public-nEUro can therefore be analysed and results merged with datasets from other institutions in order to create or improve brain atlases which might be published and shared openly (under an appropriate CCBY license). Examples of such atlases include, but are not limited to, average structural or tissue images, average molecular densities, time activity curves in regions of interest, group level covariance/connectivity matrices. In any case, only aggregated data from multiple Institutions will be used. Data analyses will take place on secured (behind firewalls with access control) private servers hosted by NRU. Only identified NRU personnel have access to the mentioned servers.

**Duration of services:**

**The Parties have agreed on the following End Date of the Agreement:**

Date:

The parties have agreed that services can be terminated earlier than the end date i) by NRU, if Institution does not pay; ii) by Institution, if a yearly payment plan is used, and updated prices do not match expectations or iii) by Institution or NRU if personal information issues become apparent in the shared dataset.

Upon the End Date of the Agreement, either a new Agreement will be drawn, or NRU will remove the Institution Data from the cloud. For the new agreement to be drawn, warm storage or archiving will be offered. Archiving still offers data access but data are not immediately available to users and can take several days. It has the advantage of offering a cheap storage solution for datasets not downloaded frequently. In the cases of data returned to Institution or a new agreement with archival, NRU will update the dataset metadata to indicate that Institution Data are from now on available only upon request from the cloud archive or directly from the Institution. If requested by Institution, the BIDS curated Institution Data can be returned to Institution.

**Payment plan:**

A one-time payment from the upload date until the agreed end date. The total requested amount is the sum of the service fees, with an annual 2% inflation adjustment, plus an additional 1,000 DKK/500GB increments to secure services in the event of sudden market price changes.

An annual payment plan. The sum requested is updated based on inflation and our subcontractor prices.

**Service fees and invoicing:**

## Invoices shall be issued to Institution via email to:

## Invoices shall be payable within thirty (30) calendar days following the invoice date, with payment being made by transferring the amount due to the bank account number stated on the invoice.

The following service fees (plus VAT, if applicable) apply:

Data instalment (includes NRU administration and PublicnEUro data management): **4000 DKK** (once)

Management and Maintenance fee, to be paid from year 2: **765\* DKK/year**

☒ Data storage \*\* **0.097\*DKK/GB/month**

*\* Prices to be adjusted for inflation and/or subcontractor storage price.*

*\*\* The curated dataset size will be rounded up to the nearest Gigabyte.*

Other optional services

BIDS-curation of pseudonymized Institution Data **1000 DKK/hour**

Open data sharing (no access control) **0 DKK**

Archiving/Cold data sharing (from tape to cloud): **1000 DKK**

(only for contract renewal)

Private hosting (additional management fee) **2000 DKK/year**

(We manage your group, and only listed people have access to as many datasets you create - adding the basic 0.97DKK/GB/month. Private hosting means there is no check from our side of datasets, i.e. no data catalogue to make them findable or BIDS validation; this is your data and files you want people in a group to be able to download).

Others (as agreed between parties): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

NRU will, on a relevant and regular basis, invoice the Institution for the services requested by the Institution and provided by NRU. Invoices will be submitted to the Institution’s contact person as defined in the Agreement. Institution will pay 100% of the invoiced amount by transferring the amount to NRU’s bank account, as indicated on the invoice, within 30 days of receipt of such invoice. Management and Maintenance fees may be updated following Danish inflation rates and Data storage cost updates as per our sub-contractor. In such cases, Institution will be contacted before sending the invoice to ensure continuity of services or appropriate termination (sections 9 and 10).

**SCHEDULE C: DATA PROCESSING AGREEMENT**

For the Data Processor’s processing of the Data Controller’s personal data related to the parties’ Agreement (‘Principal Agreement’).

Between

**NRU** (”Data Processor”)

and

**Institution** (”Data Controller”).

# Background to The Data Processing Agreement

1.1. This data processing agreement, including appendixes and any supplements (”Data Processing Agreement”), concerns the Data Processor’s obligation to act in accordance with the EU Parliament and Council’s regulation 2016/679 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, and repealing Directive 95/46/EC (“General Data Protection Regulation”), as well as legislation on supplementary provisions to the regulation 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 Law”).

1.2. The Data Processing Agreement is an integral part of the Principal Agreement.

1.3. In case of discrepancies between the provisions in the Data Processing Agreement and any corresponding provisions in other agreements between the Data Controller and the Data Processor, including the Principal Agreement, in relation to processing of personal data, the provisions in the Data Processing Agreement take precedence. This applies regardless of anything agreed about precedence elsewhere. If, however, the Data Processor is bound by more stringent obligations in other agreements between the Data Controller and the Data Processor, including the Principal Agreement, the Data Processor must fulfil those more stringent obligations.

# Data Processor’s responsibility

## 2.1.  The Data Processor must only process personal data according to documented instructions from the Data Controller, and only to the extent that is necessary for the Data Processor to fulfil the obligations of the Principal Agreement and the Data Processing Agreement, unless processing is required under EU or Member State law to which the Data Processor is subject. In this case, the Data Processor must inform the Data Controller of that legal requirement before processing, unless that law prohibits this notification on important grounds of public interest, see General Data Protection Regulation article 28, section 3, paragraph a.

2.2. The Data Processing Agreement is part of the Data Controller’s instructions to the Data Processor. The Data Processor processes personal data on behalf of the Data Controller, and must not process personal data covered by the Data Processing Agreement for own purposes, except as described in the Principal Agreement.

2.3. The Data Processor must immediately inform the Data Controller if an instruction is, in the Data Processor’s opinion, in contravention of the General Data Protection Regulation, the General Data Protection Law or the data protection provisions of EU or Member State law (combined, “General Data Protection Legislation”)

2.4. The Data Protection Agreement does not release the Data Processor from obligations directly imposed by the General Data Protection Regulation or any other current legislation.

# Data Processor’s task

The Data Processor’s processing of personal data takes place in order to fulfil the Principal Agreement.

# Technical and organisational precautions

## 4.1. The Data Processor must take all necessary measures required under article 32 of the General Data Protection Regulation. This article stipulates, among other things, 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 controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

4.2. Appendix 1 (Data Processor’s instructions) stipulates the minimum requirements for the necessary technical and organisational security measures.

4.3. The principles and recommendations in ISO 27001, with later amendments, should be used as a framework guideline for fulfilling the Data Processing Agreement requirements.

# Data Processor’s use of sub-processors

5.1. The Data Processor must not use another data processor (sub-processor) to process personal data covered by the Data Processing Agreement without the Data Controller’s prior written consent. Appendix 2 of the Data Processing Agreement lists the sub-processors approved by the Data Controller.

5.2. The Data Processor must notify the Data Controller and obtain specific written approval from the Data Controller if the Data Processor wishes to bring into use a new sub-processor. The notification must be received at least 3 months before the Data Processor wishes to bring into use the new sub-processor. The notification must take place by editing appendix 2 and sending it to the contact person.

5.3. In addition, at the request of the Data Controller, the Data Processor must provide a systemised overview of the entire chain of sub-processors mentioned in appendix 2, clearly indicating how the sub-processors are interrelated.

5.4. The Data Processor must enter into an agreement with a sub-processor which, as a minimum, complies with the data processing obligations undertaken by the Data Processor in the Data Processing Agreement. The sub-processor must have at least the same security level as undertaken by the Data Processor in the Data Processing Agreement.

5.5. If a sub-processor is used, the Data Processor must provide the relevant data processing agreement between the Data Processor and the sub-processor at the request of the Data Controller. The sub-processor must fulfil the security requirements outlined in appendix 1 (Data Processor’s instructions).

5.6. The Data Processor is responsible for the contractual and legal requirements of the sub-processor’s processing of personal data. The fact that the Data Processor enters into an agreement with a sub-processor does not release the Data Processor from the obligation to comply with the Data Processing Agreement.

5.7. The Data Processor must inform the Data Controller of termination of an agreement with a sub-processor on processing of personal data covered by the Data Processing Agreement. In this case, the Data Processor must ensure that the sub-processor properly deletes all personal data in accordance with clause 10.

5.8. In the agreement with the sub-processor, the Data Processor must, when possible, include the Data Controller as preferred third party in the event of the Data Processor’s insolvency so that the Data Controller can assume the Data Processor’s rights regarding data processing and enforce them on the sub-processor. For example, so that the Data Controller can instruct the sub-processor to delete or hand back personal data.

# 6. Transfer of personal data to third countries or international organisations

6.1. If set in the service contract by the Data Controller, the Data Processor must ensure that documented written approval (i.e. standard contractual clauses) is obtained from users located in third countries that do not ensure an adequate level of protection (article 45) when procuring access to the Data Controller’s research personal data, without having to inform the Data Controller or obtain further consent from the Data Controller. For any other cases The Data Processor must ensure that documented written approval is obtained from the Data Controller prior to the carrying out of transfers (e.g., assignment, disclosure or internal use) of personal data to third countries or international organisations unless the Data Processor is subject to other requirements under EU or Member State law. In such a case, the Data Processor must notify the Data Controller of this legal requirement before the transfer, unless the law prohibits this notification on important grounds of public interest. See General Data Protection Regulation article 28, section 3, paragraph a.

6.2. The limitations outlined in clause 6.1 mean, among other things, that the Data Processor must obtain prior written approval from the Data Controller to:

* + 1. Disclose personal data to a Data Controller in a third country or an international organisation.
    2. Assign the processing of personal data to a sub-processor in a third country or an international organisation.
    3. Allow personal data to be processed by another of the Data Processor’s departments located in a third country.

6.3. Providing that the Data Controller gives the Data Processor written consent to transfer personal data to a sub-processor in a third country, the Data Processor is responsible for ensuring that the personal data is not transferred unless there is a legal basis for transfer of personal data to the country in question. If a sub-processor in a third country is used, this must be stipulated in appendix 2 of the Data Processing Agreement.

6.4. If a transfer of personal data to a sub-processor in a third country, as outlined in clause 6.3, is based on the EU Commission’s Standard Contractual Clauses, the EU Commission’s Standard Contractual Clauses take precedence over the terms in the Data Processing Agreement for that specific transfer of personal data to the sub-processor. However, any requirements or obligations imposed on the Data Processor by the Data Processing Agreement and which are more onerous or which put the data subjects in a better position will still apply.

6.5. The Data Processor must, upon request from the Data Controller, provide any data transfer agreements entered into under the EU Commission’s Standard Contractual Clauses between the Data Processor and sub-processors.

# 7. Inspection and audit

7.1. The Data Processor must make available to the Data Controller all information necessary to demonstrate compliance with the General Data Protection Legislation and the Data Processing Agreement, and must allow for and contribute to audits and inspections carried out by the Data Controller or another auditor authorised by the Data Controller.

7.2. The Data Processor is obliged to provide the supervisory authorities which, under applicable legislation, have access to the Data Controller’s and Data Processor’s facilities, or representatives acting on behalf of the supervisory authorities, with access to the Data Processor’s physical facilities on presentation of appropriate identification. The Data Processor is similarly obliged to ensure that this type of inspection can also take place at any sub-processors.

7.3. The Data Processor is, when possible, obliged to inspect sub-processors. The Data Processor’s inspection of sub-processors must follow the agreed inspection procedure. The Data Processor must document on request that inspections of sub-processors have been carried out. Although the Data Processor is responsible for carrying out inspections of sub-processors, the Data Controller or a representative must have access to carry out inspections of sub-processors, when necessary, in the Data Controller’s professional opinion.

# 8. Notification obligation and assistance

8.1. The Data Processor is obliged to inform the Data Controller in writing and without unnecessary delay in case of any deviation from the Data Processing Agreement, for example:

* + 1. Any deviation from the instructions received.
    2. Any deviation from agreed access to personal data covered by the Data Processing Agreement.
    3. Any deviation from planned releases, upgrades, tests etc. which are relevant for the processing of personal data covered by the Data Processing Agreement.
    4. Any reasonable suspicion of confidentiality breach, misuse, loss or deterioration of personal data etc.

8.2. The Data Processor must inform the Data Controller without unnecessary delay when made aware of a personal data breach connected to the Data Processing Agreement at the Data Processor’s or at any sub-processors’ premises.

A notification of a personal data breach must include the following information:

* + 1. The nature of the personal data breach and, if possible, who is affected, the number of affected data subjects, and the number of affected personal data records.
    2. Description of the likely consequences of the breach.
    3. Description of the measures the Data Processor has taken or suggests in order to manage the personal data breach, and what can be done to limit its possible adverse effects.

8.3. The Data Processor must assist the Data Controller as much as possible with the fulfilment of the Data Controller’s obligation to respond to requests for the exercise of the data subjects’ rights under chapter 3 of the General Data Protection Regulation, by providing appropriate technical and organisational assistance without unnecessary delay, and taking into account the nature of the processing.

8.4. The Data Processor must assist the Data Controller in fulfilling obligations for which the Data Controller is responsible under relevant legislation or when assistance is necessary in order for the Data Controller to fulfil these obligations, including the obligation to carry out a data protection impact assessment.

# 9. Agreement’s commencement and duration

9.1. The Data Processing Agreement enters into effect when the Principal Agreement has been signed by both parties.

9.2. The Data Processing Agreement is in force for as long as the processing of personal data is carried out and must remain in force until processing ceases.

9.3. The Data Processor and any sub-processors are obliged to hand back or delete personal data when data processing under the Principal Agreement ceases or at the written request of the Data Controller. The Data Controller must inform the Data Processor of the time at which data processing must cease. After this, it is the Data Processor’s responsibility to hand back or delete personal data at the request of the Data Controller, and also to delete existing copies at the reported time, unless EU or Member State law requires storage of the personal data.

# 10. Processing personal data after the agreement’s termination

10.1. The Data Processor is responsible for deleting personal data in such a way that it is not possible to recover the personal data. The Data Processor is responsible for deleting personal data from any backups and any sub-processors.

10.2. When data has been deleted, the Data Processor must send a written declaration that personal data has been deleted as agreed.

10.3. If the Data Processor or any sub-processors experience insolvency, liquidation or similar and therefore cease to process personal data for the Data Controller, all personal data must be immediately handed back to the Data Controller in a way which enables the Data Controller to continue making use of it. Following this, the Data Processor, the insolvent estate or similar is obliged to delete the personal data from own systems in accordance with the above.

# Termination assistance

11.1. In the case of termination, cancellation or rescission of the Principal Agreement or the Data Processing Agreement, the Data Processor is obliged, at the request of the Data Controller, to provide termination assistance to the Data Controller until (i) all personal data has been transferred to the Data Controller in an ordinary, recognised electronic format, and (ii) the services described in the Principal Agreement have been satisfactorily handed over to the Data Controller or a new supplier selected by the Data Controller. The Data Processor must continue to process personal data and to deliver the services in accordance with the Principal Agreement until a satisfactory handover has taken place.

11.2. The Data Processor is obliged, at the request of the Data Controller, to inform the Data Controller in writing of how the Data Processor will transfer personal data and the services covered by the Principal Agreement to the Data Controller or a new supplier, including any technical requirements and conditions, so that the Data Controller or the new supplier can take over the services described in the Principal Agreement as well as the processing of personal data. The Data Processor must at the request of the Data Controller at any time be able to document and demonstrate to the Data Controller that the transfer of personal data and services can take place within the timeframe stated by the Data Processor.

# Personal data covered by this agreement is confidential.

12.1. The Data Processor must ensure and, at the request of the Data Controller, be able to demonstrate that all colleagues, sub-processors, business partners, external consultants and temporary workers etc. authorised to process the personal data covered by the Data Processing Agreement are bound by professional confidentiality or are subject to a relevant statutory duty of confidentiality.

12.2. The Data Processor is responsible for informing employees, sub-processors, business partners, external consultants and temporary workers etc. about the duty of confidentiality.

12.3. The Data Processor must ensure that access to personal data covered by the Data Processing Agreement is limited to employees who are required to process personal data in order for the Data Processor’s obligations to the Data Controller to be fulfilled. Access to personal data must therefore be blocked if authorisation is removed or expires.

12.4. The Data Processing Agreement’s obligations on confidentiality also apply after the Principal Agreement has terminated.

# Transfer

The Data Processor must not transfer the rights and obligations of the Data Processing Agreement without the Data Controller’s prior consent.

# Breach

## 14.1. In addition to the information in this clause (14), the Data Controller may invoke the usual remedies for breach provided by Danish law if the Data Processor breaches the Data Processing Agreement.

## 14.2. The Data Processing Agreement is part of the Principal Agreement, and therefore a breach of the Data Processing Agreement is also a breach of the Principal Agreement. In the case of material breach of the Data Processing Agreement, the Data Controller is entitled to cancel the Data Processing Agreement and the Principal Agreement.

## 14.3. The Data Controller’s cancellation of the Principal Agreement and the Data Processing Agreement does not mean that the Data Controller waives the right to compensation if the conditions for compensation are met.

## 14.4. Even if the Data Controller chooses not to cancel the Principal Agreement and the Data Processing Agreement on one or more occasions when entitled to do so, the Data Controller retains the right to cancel the Principal Agreement and the Data Processing Agreement on other occasions.

## 14.5. The Data Controller and the Data Processor are liable in accordance with the ordinary rules of Danish law in the event of breach of the Data Processing Agreement or violation of current General Data Protection Legislation.

If the Data Controller becomes liable to a third party, due to inter alia a claim of compensation, including a claim of compensation from the data subject(s) as a result of the Data Processor’s or any sub-processor’s breach of the Data Processing Agreement or violation of the current General Data Protection Legislation, the Data Processor must indemnify the Data Controller for all costs and losses. This is including cost and losses relating to injury caused to third party’s freedom, peace, honour or reputation.

Any liability or compensation limits determined in the Principal Agreement or elsewhere are not applicable in the case of the Data Processor’s breach of the Data Processing Agreement or violation of the current General Data Protection Legislation.

Article 82 of the General Data Protection Regulation is used to calculate compensation and other amounts payable to the data subjects as a result of a violation of General Data Protection Legislation.

The Data Processor’s obligation to indemnify the Data Controller in accordance with this section does not apply to fines or sanctions imposed on the Data Controller under article 83 or 84 of the General Data Protection Regulation.

## 14.6. The Data Controller is entitled to require the Data Processor to assist in protecting the Data Controller’s interests in any court or arbitration case, regardless of any objections the Data Processor may have about any alleged breach, as long as the Data Processor’s assistance is significant in the protection of the Data Controller’s interests, and as long as it does not harm the Data Processor’s position.

# Applicable law and jurisdiction

## The applicable law and jurisdiction are regulated separately in the Principal Agreement.

# Changes to clauses 1 - 15

## It has been necessary to make the following changes to the Data Processing Agreement : none (change if any)

# Appendixes

Appendix 1: Data Processor’s instructions

Appendix 2: Sub-processors to the Data Processor

# Appendix 1 – Data Processor’s Safety Measures

**1. Data Processor’s responsibility**

Data processing covered by the Data Processing Agreement takes place in accordance with these instructions.

**2. Data Processor’s task**

2.1 Ad hoc work premises

2.1.1. Only identified personnel has access to Institution’s data and each data access is unique (i.e. each personnel has an account and must login to access, so that operations performed on data are uniquely identifiable).

2.1.2. External IT communication connections may only be established if agreed steps are taken to ensure that unauthorised persons cannot access personal data through these connections.

**3. Technical and organisational precautions**

3.1. The Data Processor must, as a minimum, take the technical and organisational steps described below in connection with the processing of personal data covered by the Data Processing Agreement.

3.2. If more detailed technical and organisational steps are necessary to ensure compliance with clause 4 of the Data Processing Agreement, these steps must always be taken.

3.3 Security risk

3.3.1. The Data Processor must take the measures necessary to identify, evaluate and limit any reasonably foreseeable internal and external risks to the availability, confidentiality or integrity of all personal data covered by the Data Processing Agreement.

3.3.2. The Data Processor must take appropriate technical steps to limit the risk of any unauthorised access. The Data Processor must evaluate and improve the effectiveness of these precautions when necessary.

3.3.3. The Data Processor must document identified risks, as well as when a risk is reduced to an acceptable level.

The above obligation involves the Data Processor carrying out a risk evaluation followed by measures to counter identified risks. This could include any relevant measures from the following list:

a. Pseudonymisation and encryption of personal data

b. Capability to ensure continued confidentiality, integrity, availability and resilience of processing systems and services

c. Capability to correctly re-establish availability of and access to personal data in the case of a physical or technical incident

d. A procedure for regular trial, assessment and evaluation of the effectiveness of the technical and organisational measures for ensuring security of processing.

3.3.4. The Data Processor must have formal procedures for handling security incidents.

3.4. Authorisation and access control

3.4.1. Public-nEUro users data access is regulated as per Schedule B.

3.4.2. The Data Processor personnel is regulated as follow:

- Only authorised persons may access personal data processed under the Data Processing Agreement.

- The Data Processor must be able to document which employees are authorised to access personal data processed under the Data Processing Agreement.

- Only persons engaged in purposes for which the personal data is being processed may be authorised. Individual users must not be authorised for uses they do not require.

- Authorisation may also be given to persons who require access to personal data for auditing, operational or systems tasks.

-Each authorised user is provided with a personal user ID and a personal password

-The Data Processor must take steps to ensure that authorised users can only access the specific personal data they have authorisation to access.

-The Data Processor must have reasonable restrictions regarding physical access. Areas where personal data covered by the Principal Agreement is processed must be properly separated from general access areas.

-The Data Processor must have formal procedures for dealing with resetting passwords, and other situations in which the normal, logical access controls are not in force.

-There must be ongoing checks– to ensure that personnel have the access and authorisation they should have.

-The Data Processor must, without unnecessary delay, cancel access and authorisation for users who, according to a concrete evaluation, no longer require them.

3.5. Training and instruction

The Data Processor must make sure that colleagues receive adequate training and instruction to ensure that personal data is processed in accordance with relevant legislation as well as with the Data Processor’s policies and procedures.

3.6. Checks on failed access attempts and logging

All processing of personal data must be logged on hardware. The log must contain, as a minimum, information on the time, user, type of use kept for at least for 6 months, older records can be deleted unless the log’s purpose requires a longer storage period in order to use it as a tool in later investigation.

3.7. Interruption in operations

In the case of an interruption in operations, the Data Processor will inform institution if more than a week.

3.8. Disposal of equipment

3.8.1. The Data Processor must have formal procedures in accordance with best to ensure that personal data is deleted effectively before disposal of electronic equipment.

3.8.2. When disposing of equipment, the Data Processor must document the methods used, and be able to produce this documentation upon request.

4.9. Inspection

The Data Processor must carry out and document an inspection of the Data Processor’s organisation’s compliance with legal requirement, policies, procedures and this Data Processing Agreement with appendixes.

**Appendix 2 – Data Processor’s sub-processors**

The Data Processor uses the following sub-processor(s) in connection with the tasks which the Data Processor carries out for the Data Controller. By entering into the Data Processing Agreement, the Data Controller approves the use of this sub-processor.

**One appendix per sub-processor.**

|  |  |
| --- | --- |
| **Sub-processor** |  |
| Company’s full name | Technical University of Denmark |
| Company reg. number (or equivalent) | 30 06 09 46 (CVR) |
| Company address (incl. country) | Anker Engelunds Vej 101, DK-2800 Kongens Lyngby |
| Other addresses which process personal data | Computerome - DTU Risø Campus  Frederiksborgvej 399  4000 Roskilde |
| Contact person at sub-processor | Peter Løngreen, Director Computerome |
| Does the Data Processor have an agreement with the sub-processor which fulfils the requirements of the Data Processing Agreement? | Yes |
| Data processing which the sub-processor participates in | Data hosting and provide computation resources |
| Categories of personal data processed by the sub-processor | - Brain Imaging Research Data Set  - User information |

|  |  |
| --- | --- |
| **Transfer of personal data to third countries** |  |
| Does the sub-processor process personal data in a third country? | No, all data is processed in Denmark, however data can be transferred to a third country if requested by Data Controller |
| If so, list the third countries | As defined in Schedule B |
| If so, provide the legal basis for the transfer (e.g., a standard EU contract or Binding Corporate Rules) | EU Standard Contractual Clause |