RESEARCH AFFILIATION AGREEMENT

(“Agreement”)

Between

Aarhus University,

Department of [Insert name]

Address

Address

Denmark  
CVR no: 31 11 91 03

(”[Department name short]”)

and

Name of affiliate

Address

Address

(“The Affiliate”)

The Affiliate and [DEPARTMENT NAME SHORT] are also separately referred to as a “Party” and jointly as the “Parties”.

1. **BACKGROUND AND PURPOSE**
   1. The purpose of this Agreement is to regulate The Affiliate’s obligations towards [DEPARTMENT NAME SHORT] during the research collaboration for the research project: [Insert name of project] (“Project”) of [DEPARTMENT NAME SHORT]. The Affiliate commits to abide by the terms of this Agreement.
   2. [DEPARTMENT NAME SHORT] determines the purposes and means of the processing of Personal Data in the Project. The Affiliate is considered as an employee of [DEPARTMENT NAME SHORT] in regards to responsibilities for compliance with the obligations under the General Data Protection Regulation (GDPR) and thus acting under [DEPARTMENT NAME SHORT]’s direct authority.
   3. In addition to this Agreement, the conditions under which the Project shall be carried out including but not limited to publication and intellectual property rights will be regulated by the agreement entered into by and between [DEPARTMENT NAME SHORT] and [Insert name of the affiliate] (“Collaboration Agreement”). To the extent that any term of the Collaboration Agreement conflicts with any terms of this Agreement, or [DEPARTMENT NAME SHORT]’s policies and procedures applicable to The Affiliate, the term(s) of the Collaboration Agreement will supersede this Agreement and the term(s) of [DEPARTMENT NAME SHORT]’s policies and procedures.
2. **DEFINITIONS**

**Agreement:** This Agreement on the Project.

**Project:** The Project defined in clause 1.1. The Project will be conducted as part of the approved Project (Internal registration if applicable SDS:XXXX; DST: XXXXXX ; Aarhus University: [Insert number from AU’s record of processing activities])

**Collaboration Agreement:** The Collaboration Agreement defined in 1.2.

**Information Security Policy**: Aarhus University’s Information security policy and rules version 2.0 or any newer versions.

**Project Database**: [Insert specification of database at DST or SDS]

**Database Guidelines**: [Insert link to the applicable guidelines for usage of database at department or center]

**GDPR:** Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

**Data Controller**: The Data Controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law, cf. GDPR art. 4, 7.

**Data Processor:** The Data Processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller, cf. GDPR art. 4, 8). In the Project, [DST and/or SDS] will process data on behalf of AU in the Project.

**Guidelines for the Data Processor**: [Insert applicable guidelines from DST and/or SDS]

**Data Subject:** An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, cf. GDPR art. 4, 1.

**Personal Data**: Personal Data is any information relating to an identified or identifiable natural person (‘Data Subject’, cf. GDPR art. 4, 1).

**Micro Data:** Micro data are data containing, e.g.:

* Datasets or parts of datasets with information at the level of individuals – i.e. where the dataset contains a row for each individual (individual records) and also in cases where the de-identified serial number is deleted, e.g. the personal registration number. That is, a dataset at the level of individuals comprising various items of background information, e.g. income, level of education and socio-economic status, but where the de-identified personal number for each person is deleted.
* The de-identified key variables, such as personal registration numbers, CVR numbers, workplace numbers, address codes, etc. are always considered to be micro data, as they indicate a unique number referring directly to a single individual or enterprise. Even if de-identified person numbers are transferred without any other information, it is still not allowed. This applies also to external data, i.e. data which are sent to [DST and/or SDS] by the researcher and which are to be incorporated in a specific research project.

**Data Governance Expert:** New users may be granted access after supervised training and approval by a Data Governance Expert. The appointed Data Governance Expert is [Insert name or names in the department or center].

**Pseudonymised**: Pseudonymisation is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person, cf. GDPR art. 4, 5.

**VPN access:** Virtual Private Network. The VPN secures the same security level on transmission of data for your computer, as when you work at Aarhus University.

1. **FINANCE**
   1. [DEPARTMENT NAME SHORT] is not obligated to provide financial support to The Affiliate during the term of the Project, notwithstanding what is regulated in the Collaboration Agreement.
2. **RIGHTS AND OBLIGATIONS OF THE AFFILIATE**
   1. The Affiliate will during the Project have access to Personal Data.
   2. The Affiliate confirms and accepts the following technical and organizational information security measures:

* Access to Personal Data is restricted by Danish legislation. The Project must be approved before initiation, and the approval is granted to a specific Data Controller. In this case, the Data Controller is Aarhus University.
* Access to data at [DEPARTMENT NAME SHORT]’s server at Data Processor is allowed only through a personal two factor VPN access to [DEPARTMENT NAME SHORT] at Aarhus University followed by personal two factor VPN access to Data Processor.
* The personal VPN access gives access to a server located at Data Processor. This server contains the relevant Personal Data.
* To access SDS an additional NemID electronic employee signature is mandatory.
* Downloading and copying Personal Data to the researcher’s computer is neither possible nor permitted. The server is managed by Data Processor on behalf of [DEPARTMENT NAME SHORT], using strict security measures which, among others, preclude users from downloading information, modifying security settings, installing and modifying systems and/or software. All Personal Data has been Pseudonymised, but data are, according to GDPR still considered as Personal Data.
* Access to data at [DEPARTMENT NAME SHORT]’s server at Data Processor is only allowed using an Aarhus University approved computer with fully operational and updated antivirus software. [DEPARTMENT NAME SHORT] must supervise that the computer complies with the mentioned requirements.
* It is not allowed to access [DEPARTMENT NAME SHORT]’s servers at Data Processor from locations where there is any risk that any other third party may intentionally or unintentionally see the content of the screen (e.g. public areas).
* When accessing [DEPARTMENT NAME SHORT]’s servers at Data Processor the content of the screen may not be shown to persons who are not themselves granted access to the Project and the computer shall not be passed on to any other third party.
* In case of the Affiliate’s breach, anticipated breach, or any suspected or actual unauthorized use of data, [DEPARTMENT NAME SHORT] can effectively restrict or terminate all access to all data at any time during the terms of this Agreement.
* Confidential information is defined according to GDPR and the Data Processor. It applies to any information that relates to less than 5 identifiable physical persons. For business statistics, an additional confidentiality rule is applied for economic variables (e.g. turnover or value added) known as the dominance criterion. For more details, see Data Processor’s Guidelines.
* Data may not under any circumstances or with any means be extracted from [DEPARTMENT NAME SHORT]’s server at Data Processor. This also includes screen dumps, photographs, manual transcripts of the screen, video, FaceTime, Skype, or any other method.
* The password for accessing [DEPARTMENT NAME SHORT]’s server at Data Processor is strictly personal.
* All descriptive analyses and analytic modelling must be covered by the project description for the Project and only to the extent required for The Affiliate to perform the obligations relating to the Project.
* The Affiliate must participate in a course locally at [DEPARTMENT NAME SHORT] on rules for accessing and working with Personal Data. [Other additional requirements can be added]
* No attempts must be made to identify Data Subjects.
* The Affiliate must sign a contract on data access with Data Processor.
* The Affiliate may only be granted access after supervised training and approval by a Data Governance Expert.
* Extraction of results from the system is possible by contacting the appointed Data Governance Expert. Upon each extraction of data, the researcher must confirm:

1. “I asked permission to export the following result file(s) from [DEPARTMENT NAME SHORT]’s secure partition at Data Processor at the convenience of [DEPARTMENT NAME SHORT]. I am fully informed of the rules governing the export of data from Data Processor and the Project Database guidelines, Danish data protection law and GDPR, and I confirm that the results do not contain Micro Data.
2. The location of results to be exported, e.g.: [Insert location of secure landing place of data]
3. I agree and accept that in case any of the requested files do not comply with the guidelines, my possibility to export files from Data Processor will be closed for three months. Subsequent non-compliance will terminate my access to data for not less than three months”

* The Affiliate must read and comply with Aarhus University’s Information Security Policy and Project Database guidelines. Both documents must be read annually.
* The Affiliate must inform [DEPARTMENT NAME SHORT] immediately in case of The Affiliate’s breach, anticipated breach, or any suspected or actual unauthorized use of sensitive data.
* The Affiliate will only have access to data until completion of the Project or maximum two years after completion for purposes of finalization of ongoing publications.
* During the term of the Project, The Affiliate is subject to the same rules and guidelines and freedom of research applicable to other researchers employed by [DEPARTMENT NAME SHORT].
* In published articles, The Affiliate must list The Department of [Insert name], Aarhus University as an affiliation.
* Nothing grants The Affiliate the authority to bind or contract any obligation in the name of or on the account of [DEPARTMENT NAME SHORT] or to make any statements, representations, warranties, or commitments on behalf of [DEPARTMENT NAME SHORT].

1. **CONFIDENTIALITY**
   1. During the Project, The Affiliate will get access to confidential information, which includes Personal Data and proprietary information of [DEPARTMENT NAME SHORT] (“Confidential Information”).
   2. According to Danish law (Section 27, subsection 3 of the Danish Administration Act and Section 152 of the Danish Penal Code), The Affiliate is obliged to treat all Confidential Information disclosed pursuant to this Agreement strictly confidential and not to disclose the information to any third party or use the Confidential Information for its benefit or the benefit of any third party, without the prior written consent of [DEPARTMENT NAME SHORT].
   3. For the avoidance of doubt, Personal Data as defined in applicable privacy laws and their implementing regulations shall always be treated as confidential and shall be protected with an adequate level of safety and confidentiality, subject to any applicable legal, regulatory, or contractual requirements. The Affiliate’s obligation to protect Confidential Information (including Personal Data) survives any termination, cancellation, expiration, or other conclusions of this Agreement.
   4. Upon completion of the purpose for which Confidential Information is disclosed, and in the absence of further agreement between the Parties or at any time upon request, The Affiliate shall immediately cease all use and make no further use of the Confidential Information disclosed to The Affiliate and shall delete all of the Confidential Information regulated by this Agreement.
2. **TERM AND TERMINATION**

This Agreement has an effective date of DDMMYYYY (“Effective Date”) and shall continue until the expiry of The Affiliate’s participation in the Project unless the Agreement has been terminated at an earlier stage in accordance with the covenants of the Collaboration Agreement between [DEPARTMENT NAME SHORT] and [Name of affiliate].

1. **SIGNATURES**

The undersigned signify by their signature that they have agreed to the terms of this Agreement.

|  |  |
| --- | --- |
| **Aarhus University, [DEPARTMENT NAME SHORT]**  [Insert signatory name and title] | Date [insert date] |

|  |  |
| --- | --- |
|  |  |
|  | | |
| **The Affiliate**  [Insert signatory name] | Date [insert date] |