

DATA TRANSFER AGREEMENT

Between

[NAME OF THE HOSPITAL OR RESEARCH CENTRE]

(“or “**DATA PROVIDER**”)

With an address at XXXXXXXXX

And

Centre Hospitalier Universitaire Vaudois

With an address at 21 Rue du Bugnon, 1011 Lausanne, Switzerland

(“CHUV” or “**RECIPIENT**”)

Whereby the parties to this Agreement are also hereinafter collectively referred to as “Parties”.

Preamble:

The DATA PROVIDER agrees to transfer pseudonymous and/or anonymous Data to RECIPIENT, a beneficiary belonging to the Human Brain Project (HBP) / EBRAINS scientific community, and its designated ACCESS PROVIDERS. Designated ACCESS PROVIDERS are identified, for the duration of this Agreement, as ETHZ/CSCS, with its principle office address at Via Trevano 131, CH-6900, Lugano, Switzerland, hereinafter referred to as CSCS, and Akenes SA, doing business as Exoscale, with its principle office address at Boulevard de Grancy 19A, CH-1006, Lausanne, Switzerland, hereinafter referred to as EXOSCALE. The DATA PROVIDER is willing to provide such Data only to the RECIPIENT and its designated ACCESS PROVIDERS, pursuant to the terms and conditions as set forth below, and hereinafter referred to as the “Agreement”.

Definitions

- “**Human Brain Project (HBP)**”, refers to an EU funded H2020 FET Flagship Project that was launched by the European Commission's Future and Emerging Technologies (FET) scheme in October 2013 and is scheduled to run for ten years, WHEREAS its legacy will continue in EBRAINS, a sustainable European Research Infrastructure, that was launched in 2020 during HBP SGA3, the HBP's last specific grant agreement.
- “**EBRAINS**”, refers to the European Brain ReseArch INfrastuctureS (EBRAINS - Solutions for Neuroscience) that provides shared, open computing tools, models and data that serves to integrate brain science across disciplines.
- “**Data**” shall refer to a dataset with pseudonymized and/or anonymized personal health related data and information, as described in APPENDIX B of the present document, the purpose of which shall be defined by the RESEARCH. The definition of pseudonymous data is pursuant to articles 4 and 5 of the General Data Protection Regulation (hereafter referred to as GDPR) respectively pursuant to articles 25 and 26 of the Swiss Ordinance on Research on Human Being (RS 810.301) depending on the Territorial Scope of GDPR as settled under article 3 GDPR.

- **“Research”** refers to the research performed by [HOSPITAL/RESEARCH CENTRE] in the framework of the Human Brain Project / EBRAINS by using the data provided to RECIPIENT and its designated ACCESS PROVIDERS.
- **“ACCESS PROVIDER”** means a beneficiary or linked third-party that is in charge of providing access to one or more research infrastructure or installations, or part of them, as described in the Multi-Beneficiary General Model Grant Agreement of the H2020 Programme, and available under https://ec.europa.eu/research/participants/data/ref/h2020/mga/gga/h2020-mga-gga-multi_en.pdf and as specified in the Preamble here above.
- **“processing”**, shall refer to articles 2 and 4 of the GDPR respectively article 3 of the Swiss federal data protection law (RS 235.1) depending on the Territorial Scope of GDPR as settled under article 3 GDPR.

2. Object

This Agreement defines the conditions under which [HOSPITAL/RESEARCH CENTRE] agrees to provide the Data to the RECIPIENT and its designated ACCESS PROVIDERS.

2.1 [HOSPITAL/RESEARCH CENTRE] will provide RECIPIENT and its designated ACCESS PROVIDERS, as part of the framework of the Human Brain Project / EBRAINS Infrastructure, with the Data, pursuant to, and in accordance with, the conditions of this Agreement and set forth herein.

2.2 Data shall be stored and processed in accordance with the recommendations and Governance Framework of the HBP / EBRAINS infrastructure, using infrastructures and technologies operated and maintained by RECIPIENT and/or its designated ACCESS PROVIDERS or, on a case-by-case basis, by the PROVIDER. Data shall only be accessible by specific and agreed upon personnel of the PARTIES and exclusively for the purpose of Research. Data is not to be disclosed, distributed, transferred or sold by RECIPIENT or its designated ACCESS PROVIDERS, their personnel, or affiliates, to any third-party without prior written consent of [HOSPITAL/RESEARCH CENTRE]. RECIPIENT or its designated ACCESS PROVIDERS is not to use the Data in any manner for commercial purposes.

2.3 Any scientific publication which might result from the research on the data provided by [HOSPITAL/RESEARCH CENTRE] to the RECIPIENT is subject to further and separate comment by [HOSPITAL/RESEARCH CENTRE], both governing the consent of the publication, as well as the identification of the author or co-authors.

3. Compliance with Law, Rules and Regulations

RECIPIENT agrees to comply with all rules, guidelines and regulations, including but not limited to the ICH-GCP regulations and guidelines, and the Declaration of Taipei of the WMA dated October 2016, applicable to the Research and the handling, protection and use of the Data. RECIPIENT recognizes that Data shall be protected and must be processed by RECIPIENT or its designated ACCESS PROVIDERS, with protection equivalent to the Federal Act on Research involving Human Beings (RS 810.30, HRA), the Federal Act on Data Protection (RS 235.1, FADP) and with applicable local laws on data protection.

RECIPIENT agrees to immediately report (i) any actual or suspected data protection breach, including a breach against applicable data protection regulation, data protection section of this Agreement, (ii) any actual or suspected impairment or inadequacy of the RECIPIENT or its designated ACCESS PROVIDERS 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.

[HOSPITAL/RESEARCH CENTRE] warrants and represents that: (i) all applicable laws and regulations have been complied with in collecting the Data (including any information pertaining to the humans donors to be transferred to RECIPIENT or its designated ACCESS PROVIDERS, pursuant to this Agreement); (ii) ethical committee approval or equivalent approval and appropriate informed consent has been obtained and documented; (iii) the scope of the informed consent obtained from the human donors of the Data covers all aspects of the Research and any rights and licenses granted to RECIPIENT or its designated ACCESS PROVIDERS and its partners pursuant to this Agreement, and (iv) the Data will be pseudonymized and/or anonymized before being transferred to RECIPIENT or its designated

ACCESS PROVIDERS, and the key for pseudonymized data shall be kept at [HOSPITAL/RESEARCH CENTRE] in a secure manner and not be disclosed or shared with the RECIPIENT or its designated ACCESS PROVIDERS.

4. Requirements for Data protection and Data export

RECIPIENT shall not assign or subcontract the Research in whole or in part or export Data outside Switzerland or the European Union especially in territories that does not provide sufficient data protection rights in compliance of legal requirements as settled under APPENDIX C.

RECIPIENT undertakes, prior to any use or processing, any appropriate technical and organizational measures (as further described in APPENDIX D) to protect Data from any unauthorized use in accordance with the Swiss Data Protection Law (APPENDIX C) and any regulations applicable to the RECIPIENT or its designated ACCESS PROVIDERS.

RECIPIENT is not to carry out any procedures with the Data (linking, comparison, processing) with the intention to identify the concerned subject.

The Parties are responsible to ensure that the patients are provided with their right of information (right of access), correction, blocking, suppression or deletion, as provided for by any applicable legal provision including revoking their consent.

[HOSPITAL/RESEARCH CENTRE] bears the responsibility to manage the DATA, always in accordance with the appropriate consent(s), and remove any patient record from the data if the patient's consent has been revoked. This may require a full replacement of the provided data.

The Parties shall comply with the Data Processing Obligation and Undertaking as specified in APPENDIX A.

6. Ownership and Intellectual Property

- 6.1 Without prejudice of Section 8 Results of the HBP Consortium Agreement, each Party retains Ownership of its own pre-existing knowledge.
- 6.2 Ownership of all research results, patentable or not, shall be function of the inventive contribution of the participants to their achievement. In case that all or part of the analysis could be protected by a new patent application naming one or more [HOSPITAL/RESEARCH CENTRE], and RECIPIENT and its inventors, the parties shall consult each other to define the modalities of such a patent application filing, and its exploitation conditions and agree to enter into a separate joint ownership and management agreement.
- 6.3 RECIPIENT will not file, or have filed in the name of third-parties in any country, any patent application, or intellectual property rights (copyrights, trademarks, ...) claiming directly Data, or any other material that could not have been made without the Data, or manufacture or use method(s) of the Data.

7. Confidentiality Obligations

- 7.1 Any information that is identified as confidential at the time it is disclosed hereunder by [HOSPITAL/RESEARCH CENTRE] to RECIPIENT ("Confidential Information") shall be retained in confidence by RECIPIENT and its designated ACCESS PROVIDERS, and shall not be disclosed by RECIPIENT or its designated ACCESS PROVIDERS to anyone other than its employees working under its immediate control and supervision.
- 7.2 RECIPIENT'S obligations of non-disclosure and restricted use of Confidential Information shall become effective on the date of disclosure, shall apply to all Confidential Information received from [HOSPITAL/RESEARCH CENTRE] and shall survive termination of this Agreement, provided that such obligations of non-disclosure and restricted use of Confidential Information shall not extend to Confidential Information disclosed to RECIPIENT or its designated ACCESS PROVIDERS which:

- a) is or becomes part of the public domain, through no action by RECIPIENT or its designated ACCESS PROVIDERS;
- b) was in the possession of RECIPIENT or its designated ACCESS PROVIDERS at the time of disclosure and was not acquired from [HOSPITAL/RESEARCH CENTRE] under an obligation of confidentiality;
- c) was received by RECIPIENT or its designated ACCESS PROVIDERS from a third-party not under an obligation of confidentiality with respect to such information;
- d) is approved for public release by written authorization of [HOSPITAL/RESEARCH CENTRE];
- e) RECIPIENT or its designated ACCESS PROVIDERS can demonstrate was independently developed by or for RECIPIENT or its designated ACCESS PROVIDERS without using such Confidential Information;
- f) is required to be disclosed by law or court order.

8. ACCESS PROVIDERS: Usage and limitations

RECIPIENT shall be permitted to use any and all of its designated ACCESS PROVIDERS together and independently, included but not limited to, the purpose of RESEARCH. RECIPIENT shall, on a best effort basis, provide adequate security measures for the storage, transport and processing of DATA. Such measures comprise the use of encryption technologies for the storage and transport of DATA, and limit the processing to infrastructure of ACCESS PROVIDERS certified with ISO27001 or equivalent. Applicable certificates at the time of execution of AGREEMENT are listed in APPENDIX E of the present document. RECIPIENT is to notify PROVIDER of any known changes in the certification of its designated ACCESS PROVIDERS without undue delay and, where feasible, not later than TEN (10) days following the receipt and acknowledgment of the appropriate information.

9. Liability and Absence of Warranties

The Data is provided by PROVIDER "AS IS" AND [HOSPITAL/RESEARCH CENTRE] MAKES NO REPRESENTATIONS AND EXTENDS NO WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, WITH RESPECT TO THE DATA AND INFORMATION AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND OF FITNESS FOR A PARTICULAR PURPOSE OR USE. [HOSPITAL/RESEARCH CENTRE] DISCLAIMS ALL WARRANTIES OF NON-INFRINGEMENT WITH RESPECT TO ANY THIRD-PARTY RIGHTS AND TITLE, INCLUDING PATENT RIGHTS, IN THE DATA AND INFORMATION.

10. Validity and Termination

10.1 Validity

This agreement is initially valid for a period of THREE (3) years following its execution date, thereafter automatically renewed annually, unless terminated by either Party with a THIRTY (30) days notice and pursuant to point 9.2 of this agreement.

10.2 Termination

Upon completion of the Research or expiration of this Agreement or in case of early termination of this Agreement by [HOSPITAL/RESEARCH CENTRE], which may be communicated with immediate effect to RECIPIENT, for breach of this Agreement by RECIPIENT, RECIPIENT or its designated ACCESS PROVIDERS agree to discontinue use of the Data and will arrange for the return, at its charge, to [HOSPITAL/RESEARCH CENTRE] or the destruction of the remaining Data, according to the instructions of [HOSPITAL/RESEARCH CENTRE]. In case of destruction according to [HOSPITAL/RESEARCH CENTRE]'s instructions, RECIPIENT agrees to provide [HOSPITAL/RESEARCH CENTRE] free of charge with proof of such destruction.

11. Assignment

RECIPIENT shall be entitled to assign this AGREEMENT or delegate its obligations under this Agreement either in whole or in part without the prior written consent of HOSPITAL/RESEARCH CENTRE. HOSPITAL/RESEARCH CENTRE shall not assign this AGREEMENT or its obligations under this AGREEMENT without prior written approval given by RECIPIENT.

12. Modifications and Amendments

This Agreement constitutes the entire agreement and understanding of the Parties and supersedes any prior agreements or understandings relating to the subject matter hereof. This Agreement may not be modified except by a written instrument signed by all parties.

13. Governing Law and Jurisdiction

This Agreement shall be governed by the laws of Switzerland. Any claim or controversy arising out of or related to this Agreement shall be submitted to the competent courts of Canton de Vaud, Switzerland.

This Agreement may be executed in one or more counterparts, each of which when executed and delivered will be deemed to be an original, but all of which taken together will constitute one and the same agreement. This Agreement will become effective when counterparts have been signed by each of the Parties and delivered by facsimile or other means to each other Party. This Agreement may be executed and delivered by facsimile or by .pdf file and upon such delivery the facsimile or .pdf signature will be deemed to have the same effect as if the original signature had been delivered to the other Party.

[HOSPITAL/RESEARCH CENTRE]	RECIPIENT
Date:	Date:
Signature	Signature
Prof./Dr/Dre XXX [Role]	Prof./Dr/Dre XXX [Role]
Signature	Signature
Prof./Dr/Dre XXX [Role]	Prof./Dr/Dre XXX [Role]

Data Protection Particulars

The subject matter and duration of the Processing	<p>The subject matter of the Processing is the performance of the Research.</p> <p>The duration of processing is limited to the duration of the Research.</p>
The nature and purpose of the Processing	<p>The nature of the Processing is the Processing of Participant Personal Data for the purposes of performing the Research.</p>
The type of Personal Data being Processed	<p>See APPENDIX B</p>
The categories of Data Subjects	<p>The Personal Data concerns XXXXX</p>

APPENDIX A: Data processing obligations and undertaking in line with applicable data protection laws and regulations in Switzerland within the European Union

DEFINITIONS

Data Protection Legislation means any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (as amended, consolidated or re-enacted from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which a Party is subject, including the Federal Act on Data Protection and the General Data Protection Regulation ((EU) 2016/679) (“**GDPR**”) and all applicable national data protection laws and regulations.

Data Controller, Data Processor, Data Subject, and Processing (and variations thereof) have the meanings set out in the Data Protection Legislation.

Personal Data means any personal data (as defined in the Data Protection Legislation) Processed by either Party in connection with this Agreement and the Clinical Trial Agreement.

1. DATA PROTECTION

- 1.1 Both Parties will comply with all applicable requirements of the Data Protection Legislation. This Clause (Data Protection) is in addition to, and does not relieve, remove or replace, a Party's obligations under the Data Protection Legislation.
- 1.2 The Parties acknowledge that for the purposes of the Data Protection Legislation, [HOSPITAL/RESEARCH CENTRE] is the Data Controller and CHUV is the Data Processor.
- 1.3 To the extent that the CHUV Processes any Personal Data as a Data Processor for and on behalf of the [HOSPITAL/RESEARCH CENTRE] (as the Data Controller) it shall:
 - 1.3.1 only process pseudonymous and/or anonymous Personal Data for and on behalf of the [HOSPITAL/RESEARCH CENTRE] for the purposes of performing its obligations under this Agreement and only in accordance with the [HOSPITAL/RESEARCH CENTRE]'s written instructions from time to time, unless the CHUV is required to follow applicable law to process pseudonymous and/or anonymous Personal Data. In such a case, the CHUV shall inform the [HOSPITAL/RESEARCH CENTRE] of that legal requirement before Processing, unless the law prohibits such information on important grounds of public interest;
 - 1.3.2 inform the [HOSPITAL/RESEARCH CENTRE] immediately if it considers any of the [HOSPITAL/RESEARCH CENTRE]'s instructions to be infringing Data Protection Legislation;
 - 1.3.3 ensure that [RECIPIENT] and its designated ACCESS PROVIDERS have in place appropriate technical and organisational measures in compliance with APPENDIX D, sufficient to comply at least with the obligations imposed on the Controller by applicable data protection laws, to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it);
 - 1.3.4 ensure by signature of respective agreements that any persons who have access to and/or Process Personal Data are obliged to keep the Personal Data confidential;

- 1.3.5 taking into account the nature of the Processing, at the [HOSPITAL/RESEARCH CENTRE]'s request, assist the [HOSPITAL/RESEARCH CENTRE] to comply with the obligations imposed on the [HOSPITAL/RESEARCH CENTRE] by the Data Protection Legislation in relation to: (i) security, breach notifications, data protection impact assessments, and consultations with supervisory authorities or regulators; and (ii) responding to any requests from Data Subjects.
- 1.3.6 notify the [HOSPITAL/RESEARCH CENTRE] promptly following its receipt of any request from a Data Subject to exercise their rights under the Data Protection Legislation or any correspondence from a supervisory authority or regulator and shall:
- (i) not disclose any Personal Data without first consulting with and obtaining the [HOSPITAL/RESEARCH CENTRE]'s prior written consent; and
 - (ii) provide the [HOSPITAL/RESEARCH CENTRE] with all reasonable co-operation and assistance required by the [HOSPITAL/RESEARCH CENTRE] in relation to any such request or correspondence;
- 1.3.7 notify the [HOSPITAL/RESEARCH CENTRE] without undue delay and in any event within twenty-four (24) hours) upon becoming aware of any Personal Data breach, and:
- (i) conduct or support the [HOSPITAL/RESEARCH CENTRE] in conducting such investigations and analysis that the [HOSPITAL/RESEARCH CENTRE] reasonably requires in respect of such breach;
 - (ii) implement any measures necessary to restore the security of compromised Personal Data; and
 - (iii) assist the [HOSPITAL/RESEARCH CENTRE] to make any notifications to supervisory authorities or regulators and affected Data Subjects;
- 1.3.8 keep a record of any Processing of the Personal Data it carries out on behalf of the [HOSPITAL/RESEARCH CENTRE] and hold the Personal Data in such a manner that it is capable of being distinguished from other data or information processed by [HOSPITAL/RESEARCH CENTRE];
- 1.3.9 promptly comply with any request from the [HOSPITAL/RESEARCH CENTRE] to amend, transfer or delete any Personal Data;
- 1.3.10 at the written direction of the [HOSPITAL/RESEARCH CENTRE], delete or return Personal Data and copies thereof to the [HOSPITAL/RESEARCH CENTRE] upon termination of the Agreement unless required by applicable law to store the Personal Data;
- 1.3.11 at the [HOSPITAL/RESEARCH CENTRE]'s reasonable request:
- (i) make available to the [HOSPITAL/RESEARCH CENTRE] evidence to demonstrate the [HOSPITAL/RESEARCH CENTRE]'s compliance with the requirements of this Clause; and
 - (ii) allow for and contribute to audits, including inspections, conducted by or on behalf of the [HOSPITAL/RESEARCH CENTRE], on reasonable notice and subject to appropriate confidentiality obligations;
- 1.3.12 not engage a third-party processor of Personal Data under this Agreement (a sub-processor) unless the [HOSPITAL/RESEARCH CENTRE] in its absolute discretion gives a specific or general written authorisation; and where such consent is given, the CHUV:
- (i) shall inform the [HOSPITAL/RESEARCH CENTRE] of any intended changes to a general written authorisation to add or replace processors, thereby giving the [HOSPITAL/RESEARCH CENTRE] the opportunity to object to such changes;

- (ii) impose data protection obligations that are substantially the same to those set out in this Agreement;
 - (iii) acknowledges that the CHUV remains fully liable to the [HOSPITAL/RESEARCH CENTRE] for the performance of any sub-contracted Processing obligations,
- 1.3.13 not transfer any Personal Data outside Switzerland or outside of the European Economic Area (“EEA”) or to an international organisation¹ except:
 - (i) with the prior written consent of the [HOSPITAL/RESEARCH CENTRE] and in accordance with any written instructions and terms the [HOSPITAL/RESEARCH CENTRE] may impose on such transfer to ensure that transfers of Personal Data outside of the EEA have adequate protections in place as set out in the Data Protection Legislation; or
 - (ii) if required by applicable law, in which case the CHUV shall inform the [HOSPITAL/RESEARCH CENTRE] of that legal requirement before transferring, unless the law prohibits such information on important grounds of public interest.
- 1.4 Notwithstanding anything in the Agreement to the contrary, this Clause (Data Protection) shall continue in full force and effect for so long as the Processor processes any Personal Data.

¹ Defined as an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries (GDPR Article 4(26))

APPENDIX B: Detailed descriptions

This agreement permits the update of the provided data as maybe necessary from time to time so long as the nature of such update corresponds to the object and the research as established and defined in the agreement.

Data shall mean:

Please review and PROVIDE A DETAILED DESCRIPTION OF THE DATA in **Appendix B1** for the Medical Informatics Platform (MIP) and/or **Appendix B2** for the Human intracerebral EEG Platform (HIP).

APPENDIX C - Federal Act on Data Protection (RS 235.1, FADP)**Art. 6 Cross-border disclosure**

1 Personal data may not be disclosed abroad if the privacy of the data subjects would be seriously endangered thereby, in particular due to the absence of legislation that guarantees adequate protection.

2 In the absence of legislation that guarantees adequate protection, personal data may be disclosed abroad only if:

- a. sufficient safeguards, in particular contractual clauses, ensure an adequate level of protection abroad;
- b. the data subject has consented in the specific case;
- c. the processing is directly connected with the conclusion or the performance of a contract and the personal data is that of a contractual party;
- d. disclosure is essential in the specific case in order either to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts;
- e. disclosure is required in the specific case in order to protect the life or the physical integrity of the data subject;
- f. the data subject has made the data generally accessible and has not expressly prohibited its processing;
- g. disclosure is made within the same legal person or company or between legal persons or companies that are under the same management, provided those involved are subject to data protection rules that ensure an adequate level of protection.

3 The Federal Data Protection and Information Commissioner (the Commissioner, Art. 26) must be informed of the safeguards under paragraph 2 letter a, and the data protection rules under paragraph 2 letter g. The Federal Council regulates the details of this duty to provide information.

Federal Act on Research involving Human Beings (RS 810.30, HRA)**Art. 42 Export**

1 Genetic data may be exported for research purposes if informed consent has been given by the person concerned. For consent, Articles 16 and 22-24 and 32 apply *mutatis mutandis*.

2 Non-genetic health-related personal data may be disclosed abroad for research purposes if the requirements specified in Article 6 of the Federal Act of 19 June 1992 on Data Protection are met.

(non official English version)

Art. 17 Cross-border communication of data

¹ The communication to a third country of personal data undergoing processing or intended for processing may only take place if the third country in question ensures an adequate level of protection.

² The preceding paragraph is not applicable:

if the data subject has given his or her consent, which must in any case be explicit;

if the communication of data is necessary for the performance of a contract between the data subject and the controller or for the performance of pre-contractual measures taken at the request of the data subject;

if the communication is necessary for the conclusion or performance of a contract concluded or to be concluded, in the interest of the data subject, between the controller and a third-party;

if the disclosure is, in the present case, essential either to protect a public interest or to establish, exercise or defend a legal claim;

if the communication is, in the present case, necessary to protect the life or physical integrity of the person concerned;

if the communication is made from a public register which, by virtue of legal or regulatory provisions, is intended to inform the public or any person proving a legitimate interest, insofar as the legal conditions for consultation are fulfilled in the particular case;

if sufficient guarantees, in particular contractual guarantees, permit to ensure an adequate level of protection abroad.

APPENDIX D - Minimal Security Requirement

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

- deny unauthorized persons access to facilities and data processing systems;
- prevent unauthorised persons 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 or if, when and by whom data was modified or removed;
- ensure adequate organisational measures 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 the DATA PROVIDER;
- 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 the persons involved in the processing of data diligently and appropriately, by implementing and enforcing adequate confidentiality and data protection guidelines, by running regular data protection and privacy trainings, and by documenting all the organisational measures;
- guarantee that the efficacy of technical and organisational measures is regularly reviewed and assessed.
- Implement corrective measures and automatic reporting in case of any suspected data security breach

APPENDIX E: Applicable certificates at the time of execution of AGREEMENT

Exoscale-CSA_STAR_2-security-certificate

Exoscale-ISO27001-security-certificate

Exoscale-ISO27018-security-certificate