



AGREEMENT ON COLLABORATION IN THE AREA OF RESEARCH

Mayo Clinic Arizona and St. Anne's University Hospital – International Clinical Research Center

AMENDMENT #4

Joint Controller General Data Protection Regulation Data Processing Addendum for The Agreement on Collaboration in the Area of Research

Mayo Clinic Arizona and St. Anne's University Hospital – International Clinical Research Center (European Economic Area & Switzerland)

This Joint Controller Data Processing Addendum (this "*Addendum*") is part of The Agreement on Collaboration in the Area of Research ("*Agreement*") between the **International Clinical Research Centre of St. Anne's University Hospital in Brno (Fakultní nemocnice u sv. Anny v Brně)**, having a principal place of business at Pekarska 53, 65691, Brno, Czech Republic ("*Joint-Controller FNUSA-ICRC*") and **Mayo Clinic Arizona**, an Arizona charitable corporation, located at 13400 East Shea Boulevard, Scottsdale, AZ 85259 and its Affiliates ("*Joint-Controller Mayo Clinic*") and governs Joint-Controller's Processing of Personal Data in connection with Joint-Controller's conduct of the studies and performance of their other obligations as described in the Agreement ("*Study Conduct*"). Except as expressly stated otherwise, in the event of a conflict between the terms of the Agreement and the terms of this Addendum, the terms of this Addendum will take precedence with respect to GDPR compliance matters. The Addendum will be effective on the last signature date set forth below.

The Parties agree that for the purposes of this Addendum, the Parties are Joint Controllers, as that term is understood under GDPR Article 26. The shares in responsibility are defined more specifically in each project plan, protocol, informed consent form, etc.

1. Definitions. Capitalized terms used, but not otherwise defined, in this Addendum shall have the meanings given to them in Regulation (EU) 2016/679, the General Data Protection Regulation or the Agreement.

"**GDPR**" means Regulation (EU) 2016/679, the General Data Protection Regulation.

"**Personal Data**" means any information relating to an identified or identifiable natural person in the European Economic Area ("**EEA**") or Switzerland ("**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. The wording “Personal Data” includes Special Categories of Personal Data.

“Special Categories of Personal Data” means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, Genetic Data, Biometric Data for the purpose of uniquely identifying a natural person, Data Concerning Health or data concerning a natural person’s sex life or sexual orientation.

“Data Concerning Health” means Personal Data of a Special Category related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

“Genetic Data” means Personal Data of a Special Category relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or provision of access to Personal Data transmitted, stored, or otherwise Processed.

“Processing” means any operation or set of operations that is performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation in the form of disclosure of Personal Data, or their other use, disclosure by transmission, dissemination, or otherwise making available and dissemination of Personal Data, alignment or combination, restriction, erasure, or destruction. **“Process of Personal Data”** and **“Processed Personal Data”** will have a corresponding meaning.

2. Compliance with Applicable Law. Each Party shall comply with all applicable provisions of EU and internal Member State privacy and data protection laws to which the Party is subject, including but not limited to provisions relating to engagement of Processors. At present, both Parties as Joint-Controllers declare, that they do not involve any external Processor in Processing concerning the Personal Data transmitted by the other Party (Joint-Controller), and if such need arises in the future, the engagement of any Processor will be subject to prior written authorization of the other Party (Joint-Controller), who is a Data Exporter. Since Joint-Controller Mayo Clinic is acting as a Controller within the EU, Mayo Clinic will comply with, and will be subject to, the GDPR, although it may also be subject to U.S. laws (e.g., the Health Insurance Portability and Accountability Act) and must comply with the U.S. law as well. As stated in the Agreement (Section 3.04), should the collaborative research involve processing of patient data originating in the European Union (EU), respective EU rules on Personal Data processing shall be observed by the Parties, which may include also the obligation of both Parties to conclude a separate agreement on the transfer of Personal Data to the USA. Mayo Clinic Principal Investigators shall be responsible for informing FNUSA-ICRC of applicable U.S. laws concerning patient data; FNUSA-ICRC Principal Investigators shall be responsible for informing Mayo Clinic of applicable EU laws concerning patient data. Any processing of patient data shall be always subject to the strictest laws and regulations applicable to that Party.

3. Obtaining Consent. Joint-Controllers will each obtain consent from Data Subjects for the Processing of the Personal Data by the Party, as required by GDPR Article 7 or Article 9, as applicable. At the point of obtaining consent, Joint-Controllers will cooperate to notify Data Subjects of each Party’s role with respect to Processing of the Data Subject’s Personal Data.

4. Data Subject Rights. The Parties will maintain appropriate technical and organizational measures needed to enable them to respond to requests from Data Subjects exercising the Data Subjects' rights in Chapter III of the GDPR with respect to any relevant Personal Data held by the Parties ("**Request**"). The Parties will cooperate efficiently in connection with a Request. A Party receiving a Request will promptly inform the other Party if it is unable to fulfill the Request. The Parties will work in good faith to resolve the Request within the deadlines specified by the GDPR and to determine whether there exist any derogations to a data subject's rights set forth in Chapter III of the GDPR.

5. Data Transfers Outside of the EEA. To the extent that the Study Conduct involves a transfer of Personal Data originating from either Party's systems in the EEA or Switzerland to either Party's systems located in countries outside the EEA or Switzerland that have not received a binding adequacy decision by the European Commission, such transfers are subject to applicable data transfer mechanisms, such as Standard Contractual Clauses ("SCC"). The Parties have executed the SCCs, attached hereto in Exhibit A of this Addendum. Within those SCCs, Joint-Controller Mayo Clinic has chosen in Section II(h) option (iii), agreeing to process the Personal Data in accordance with the data processing principles set forth in Annex A of the SCC.

Generally, the Parties of the Agreement on Collaboration in the area of Research and the respective GDPR Addendum recognize that the Data generated and shared by the Parties hereunder should be, if technically possible, *de-identified* under HIPAA (45 C.F.R. 164.514) and *pseudonymized* (Art. 4 point 5 of GDPR). The Parties agree that the *pseudonymizational key* or other *identifier* shall not be shared with the other Party. The Parties agree to notify the Principal Investigators concerning the terms of this section.

6. Recordkeeping. Upon a request issued by a Supervisory Authority to either Party for records regarding Personal Data, the Party receiving the request will respond, with the other Party's collaboration and assistance, to the Supervisory Authority and the other Party will cooperate and provide the responding Party with records related to Processing activities performed on behalf of the other Party, including information on the categories of Personal Data Processed and the purposes of the Processing, the use of Processors with respect to such Processing, any disclosures of Personal Data to third parties, transfers of Personal Data to third countries and documentation on suitable safeguards to protect such Personal Data, and a general description of technical and organizational measures to protect the security of Personal Data.

7. Retention. Personal Data received by either Party in connection with the Agreement will be retained only for so long as may be reasonably required in connection with the Parties' performance of the Agreement or as otherwise required under applicable law or regulation to which the Joint-Controllers are subject. The specific length of time that data will be maintained and used for each project will be defined in the protocol of each project or study. Upon termination of the Agreement and this Addendum, each Party will promptly securely dispose of all Personal Data and delete existing copies unless applicable law or regulation to which the Joint-Controllers are subject requires storage or retention of the Personal Data.

8. Breach Notification. After becoming aware of a Personal Data Breach, each Party will notify the other Party without undue delay of: (a) the nature of the data breach; (b) the number and categories of data subjects and data records affected; (c) the name and contact details for the relevant contact person; (d) description of the likely consequences of the Personal Data Breach; and description of the measures taken or proposed to be taken to address the Personal Data Breach, including where appropriate, measures to mitigate its possible adverse effects. Each Party will also promptly provide the other Party such other information as the Party may reasonably request,

including, but not limited to documentation of its investigation. The Party responsible for the Personal Data Breach shall promptly inform the other Party, i. e. the other Joint-Controller. This obligation doesn't impact the legal obligation of Joint-Controller FNUSA-ICRC stipulated by GDPR to be responsible for providing notifications required by GDPR to Czech Supervisory Authority within 72 hours in case of Personal Data Breach concerning Data Subjects on the Czech territory and possible notification to Data Subjects, when the Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons. The Party responsible for the Personal Data Breach shall use its best efforts to promptly provide the other Party with an opportunity to review and approve any breach notification which mentions that Party. To the extent the Parties are jointly responsible for a Personal Data Breach, the Parties agree to work collaboratively to determine the manner of such notification and an equitable apportionment of notification costs and costs of remediating and/or mitigating the Personal Data Breach, taking into account the relative fault of the Parties.

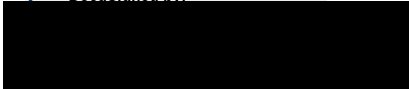
9. Survival. All obligations of the Parties concerning their cooperation in the event of an audit(s) carried out by the authorities in the USA or in the Czech Republic set forth in this Addendum shall survive termination or expiration of this Addendum and the Agreement indefinitely.

The Parties' authorized signatories have duly executed this Addendum as of the dates set forth below.

FNUSA

MAYO CLINIC ARIZONA

Signature: _____


Signature: _____
DocuSigned by:


Title: Director

Title: Director, Legal Contract Administration

Name: Ing. Vlastimil Vajdák

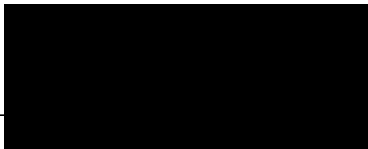
Name: 

Date: 22.10.2019

Date: 9/25/2019

FNUSA-ICRC

Signature: _____


Signature: _____


Title: ICRC Principal Investigator

Title: Mayo Principal Investigator

Name: 

Name: 

Date: 30.10.2019

Date: 9/25/2019



Joint-Controller FNUSA-ICRC Notification
(Contact details):

Data Protection Officer
St. Anne´ University Hospital in Brno
Pekařská 664/53
656 91 Brno, Czech Republic
Phone: (00420) 534 184 070
(00420) 731 416 981
Fax: (00420) 534 183 285
E-mail: dpo@fnusa.cz

Joint-Controller Mayo Clinic Notification
(Contact details):

Mayo Clinic Data Privacy Officer
200 First Street SW
Rochester, MN 55905
Phone: (507) 266-6286
Fax: (507) 538-3501
E-mail:
DLEnterprisePrivacyOffice@mayo.edu

Copy to:
Mayo Clinic Legal Department
200 First Street SW
Rochester, MN 55905
Fax: (507) 284-0929

EXHIBIT A

Standard Contractual Clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)



EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
Unit C.3: Data protection

Commission Decision C(2004)5721

SET II

**Standard contractual clauses for the transfer of personal data from the
Community to third countries (controller to controller transfers)**

**In conjunction with the Collaboration in the Area of Research Agreement
between the parties identified below (“Agreement”), the parties agree as follows:**

Data transfer agreement

between

**International Clinical Research Centre of St. Anne’s University Hospital in Brno
(Fakultni nemocnice u svate Anny v Brne) (name)**

Pekarska 53, 65691

Brno, Czech Republic (address and country of establishment)

hereinafter “data exporter”)

and

Mayo Clinic Arizona (name)

13400 East Shea Boulevard

Scottsdale, AZ 85259 United States of America (address and country of
establishment)

hereinafter “data importer”

each a “party”; together “the parties”.

Definitions

For the purposes of the clauses:

- (a) “personal data”, “special categories of data/sensitive data”, “process/processing”, “controller”, “processor”, “data subject” and “supervisory authority/authority” shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby “the authority” shall mean the competent data protection authority in the territory in which the data exporter is established);

- (b) “the data exporter” shall mean the controller who transfers the personal data;
“the data importer” shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country’s system ensuring adequate protection;
- (d) “clauses” shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in **Annex B**, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

- (a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.
- (b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.
- (c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.
- (d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.
- (e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

- (a) It will have in place appropriate technical and organizational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized

disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

- (b) It will have in place procedures so that any third party it authorizes to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorized or required by law or regulation to have access to the personal data.
- (c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.
- (d) It will process the personal data for purposes described in **Annex B**, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.
- (e) It will identify to the data exporter a contact point within its organization authorized to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).
- (f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).
- (g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion. Any audit or review under this clause will be subject to conditions that the data importer reasonably requests to protect the confidentiality of its data files, documentation, and/or other information of a confidential or proprietary nature.
- (h) It will process the personal data, at its option, in accordance with:
 - (i) the data protection laws of the country in which the data exporter is established, or
 - (ii) the relevant provisions (1) of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such

an authorization or decision and is based in a country to which such an authorization or decision pertains, but is not covered by such authorization or decision for the purposes of the transfer(s) of the personal data⁽²⁾, or

(iii) **the data processing principles set forth in Annex A.**

Data importer to indicate which option it selects: (iii)

Initials of data importer: amc

- (i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and
- (i) the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or
 - (ii) the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or
 - (iii) data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or
 - (iv) with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III. Liability and third party rights

- (a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.
- (b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

- (a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.
- (b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes. The parties agree that the foregoing shall not negate, alter, or supersede any dispute resolution procedure between the parties set forth in the Agreement, and that in the event of a dispute between the data importer and the data exporter concerning any alleged breach of any provision of these clauses, such dispute shall be handled in accordance with the dispute resolution procedure (if any) set forth in the Agreement.
- (c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

- (a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.
- (b) In the event that:
 - (i) the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);
 - (ii) compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;
 - (iii) the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;
 - (iv) a final decision against which no further appeal is possible of a competent court of the data

exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

(v) a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

(c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

(d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

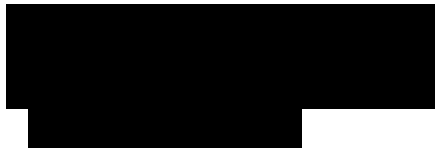
VII. Variation of these clauses

The parties may not modify these clauses except to update any information in **Annex B**, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

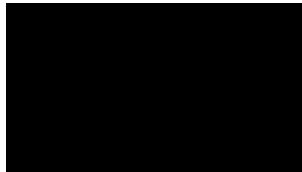
VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in **Annex B**. The parties agree that **Annex B** may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. **Annex B** may, in the alternative, be drafted to cover multiple transfers.

Dated: September 25, 2019



Director, Legal Contract Administration
9/25/2019



FOR DATA EXPORTER



Ing. Vlastimil Vajdák

Director, St. Anne's University Hospital in Brno
22.10.2019

ANNEX A

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in **Annex B** or subsequently authorized by the data subject.
2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.
3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.
4. Security and confidentiality: Technical and organizational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.
5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organization holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organizations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organization may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6.Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7.Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes.

8.Automated decisions: For purposes hereof “automated decision” shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

(a)(i) such decisions are made by the data importer in entering into or performing a contract with the data subject, and

(ii) (the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

or

(b) where otherwise provided by the law of the data exporter.

ANNEX B

DESCRIPTION OF THE TRANSFER

(To be completed by the parties)

Data Subjects

The personal data transferred concern the following categories of data subjects:

Clinical research subjects participating in research projects conducted by the parties

Purposes of transfer(s)

The transfer is made for the following purposes:

To permit the data importer (Mayo Clinic) to analyze personal data for purposes of research projects conducted by the parties

Categories of data

The personal data transferred concern the following categories of data:

demographic data of research subjects and such other research data that is not sensitive data as described below

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients:

Personnel at data importer (Mayo Clinic) who will be processing the data for the purposes described above

Sensitive data (if appropriate)

The personal data transferred concern the following categories of sensitive data:

research data may include data revealing racial or ethnic origin, genetic data, biometric data, and/or data concerning health

Data protection registration information of data exporter (where applicable)

Additional useful information (storage limits and other relevant information)

Contact points for data protection enquiries

Data importer

[REDACTED]

Privacy Officer

Mayo Clinic

Email: [REDACTED]

Phone: [REDACTED]

Data exporter

[REDACTED] a

Data Protection Officer

St. Anne's University Hospital in Brno

Email: dpo@fnusa.cz

Phone: (00420) 534 184 070