**Data Transfer Agreement**

**Agreement relating to the Intra-Group Transfer of Personal Data in Accordance with Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data Based on EC Commission Decision (204/915/EC) of December 27, 2004**

This Data Transfer Agreement (“**Agreement**”) is entered into by *[IU Consulting and Research Germany GmbH (“****Data Exporter****”)] and [Indiana University (“****Data Importer****”)]* (each a “**Party**” and collectively the “**Parties**”).

**Preamble**

Whereas, the Parties wish to exchange certain information for purposes described in more detail below;

Whereas, such an exchange of information involves transfers of personal data;

Whereas, the personal data transferred is described in Annex B to this Agreement;

Whereas, the Parties wish to adduce adequate safeguards in connection with such transfers of personal data with respect to the protection of privacy and fundamental rights and freedoms of the data subjects;

Whereas, European data protection laws require data exporters in EU/EEA countries to provide adequate protection for transfers of personal data to non-EU/EEA countries and such protection can be adduced by requiring the data importers to enter into the Standard Contractual Clauses for the Transfer of Personal Data to Third Countries (“**Model Contract**”) pursuant to Commission Decision 2004/915/EC of December 27, 2004;

Whereas, the Model Contract must be slightly modified (e.g., in terms of terminology).

NOW, THEREFORE, in order to enable the Parties to continue their relationship in a manner that is compliant with law and for other good and valuable consideration, the receipt of which is+ hereby acknowledged, the Parties have entered into this Agreement as follows:

**MAIN DOCUMENT**

1. **Document structure and hierarchy**
	1. This Agreement consists of various parts:

This Main Document contains general provisions regarding the structure of the Agreement, the hierarchy of the different parts of the Agreement, terms used in the Agreement, procedures for changes to this Agreement, and other items.

Appendix 1 contains the unmodified Model Contract.

Annex A contains the data processing principles applicable to all transfers of personal data covered hereunder.

Annex B contains a description of the transfer of personal data transferred to Company.

Appendix 2 contains a description of the data security measures.

Appendix 3 contains local law amendments to this Agreement.

* 1. The clauses of Appendix 1 (including its Annexes) shall prevail over any conflicting clauses in the remainder of the Agreement, unless specified otherwise in Appendix 3.
	2. The following terms defined and used in Appendix 1 shall be interpreted as follows:

“**data exporter**” shall be understood as referring to the relevant data exporter;

“**data importer**” shall be understood as referring to the relevant data importer.

1. **Changes to this Agreement**

2.1 Unless this Agreement expressly permits a different form, any change to this Agreement must be made in writing in order to be effective. The same shall apply to any waiver of this written form requirement.

2.2 At any time during the term of the Agreement, either Party may request, and the other Party shall agree to, such changes to the Agreement that are necessary for data protection compliance.

1. **Miscellaneous**

3.1 Save as provided otherwise in Appendix 1, nothing in this Agreement is intended to establish, or shall be construed as establishing, joint and several liability, and no Party shall be liable for acts or omissions of another Party.

3.2 Should any provision of this Agreement be or become invalid or unenforceable in whole or in part, this shall not affect the validity of the remainder of this Agreement. The invalid or unenforceable provision shall automatically be replaced by a valid and enforceable provision that comes closest to the intention and purpose of the original provision. This rule shall apply analogously if the Agreement contains an unintended gap.

3.3 Only the English language version of this Agreement shall be binding.

3.4 Any reference made in Appendix 1 to the “clauses” shall be understood as relating to all provision of this Agreement, unless otherwise provided herein. By way of example, the choice of law contained in Appendix 1, clause IV, shall not only apply to Appendix 1 but to the entire Agreement.

**Signatures**

**Data Exporter**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Place, date Name

**Date Importer**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Place, date Name

**APPENDIX 1**

**STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA FROM THE COMMUNITY TO THIRD COUNTRIES (CONTROLLER TO CONTROLLER TRANSFERS) - SET II**

**Definitions**

For the purposes of the Clauses:

1. “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 October 24, 1995 (whereby “the authority” shall mean the competent data protection authority in the territory in which the data exporter is established);
2. “the data exporter” shall mean the controller who transfers the personal data;
3. ‘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;
4. “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.

1. **OBLIGATIONS OF THE DATA EXPORTER**

The data exporter warrants and undertakes that:

1. The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.
2. It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.
3. 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.
4. It will respond to enquiries from data subjects and the authority concerning processing of the personal data by 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.
5. It will make available, upon request, a copy of the clauses to data subject 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 subject, 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.
6. **OBLIGATIONS OF THE DATA IMPORTER**

The data importer warrants and undertakes that:

1. 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.
2. 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.
3. 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.
4. It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfill the undertakings set out in these clause.
5. 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).
6. At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfill its responsibilities under clause III (which may include insurance coverage).
7. 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 object 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.
8. It will process the personal data, at its option, in accordance with:
9. The data protection laws of the country in which the data exporter is established, or
10. The relevant provisions of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provision 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, or
11. The data processing principles set forth in Annex A.

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

Initials of data importer: (see signature lines)

1. 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
2. The third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or
3. 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
4. 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
5. With regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer.
6. **LIABILITY AND THIRD PARTY RIGHTS**
7. 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.
8. 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€, 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 allegation 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 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).
9. **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.

1. **RESOLUTION OF DISPUTES WITH DATA SUBJECTS OR THE AUTHORITY**
2. 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 of claims, and will cooperate with a view to settling them amicably in a timely fashion.
3. 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.
4. 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.
5. **TERMINATION**
6. 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.
7. In the event that:
8. 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);
9. Compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;
10. The data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;
11. 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
12. 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.
13. 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 iii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.
14. 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.
15. **VARIATION OF THESE CLAUSES**

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.

**SIGNATURES**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Place/date Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Place/date Name

**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 data subjects: 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 interest 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. 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. Under certain conditions, a data subject must finally be able to receive the personal data concerning him, which he has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller. 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 direct 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:
	1. (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 the parties.

Or

* 1. Where otherwise provided by the law of the data exporter.

**SIGNATURE**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Place/date Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Place/date Name

**APPENDIX 2**

**Documentation of Data Protection Measures**

The documentation of data protection measures and data security is made in the context of Annex A of the EU Standard Contractual Clauses for the “Companies Annex B” data transfer.

You can document the required information in part or entirely with already existing documents and is not bound by the form of this questionnaire. If necessary a reference to the relevant documentation should be entered in the questionnaire.

1. **Organizational Information**
	1. Information on training and staff awareness about data protection
	2. *What written rules exist to protect the data? (for example Privacy Policy, IT Security Policies, Acceptable Use agreement, etc.)*
2. **Technical and Organizational Measures**

* 1. Entry control (facility)

*What measures ensure that only authorized personnel has access to the rooms with data processing systems? [Examples: Entry control systems, ID card readers, magnetic cards, chip cards/keys/key issuing, door security, concierges, monitoring equipment, alarm system.]*

* 1. Access control

*What measures ensure that no data processing systems are used by unauthorized persons? What measures are in use to discover an unauthorized use of data processing systems? [Examples: Password procedure (e.g. special characters, minimum length, regularly changing the password), automatic blocking, setting up a user master record set per user, encryption of data storage media.]*

* 1. Data access control

*What measures ensure that users can only access the personal data to which their access authorization refers, and that during processing, this data cannot be read, copied, changed or removed without authorization. [Examples: Differentiated permissions (profiles, roles, transactions and objects), analysis, information, changing, deletion.]*

* 1. Transfer control

*What measures ensure that ensure that personal data, during electronic transmission, data transport or saving on data storage media, cannot be read, copied, changed or removed without authorization? [Examples: Encryption via a virtual private network, electronic signature, logging, transport safety.]*

* 1. Input control

*How do you ensure that any manipulation or changes to the personal data of the principal will be recognized? [Examples Logging and log analysis systems]*

* 1. Order control

*Measures to guarantee that when an order is given to process personal data, it can only be done according to the instructions of the Principal. [Examples: Clearly drafted contract, formalized order placing (order form), criteria for selecting the Contractor, check on contract execution.]*

* 1. Availability Control

*Measures for data security shall be described such as antivirus, firewall, contingency planning, backup, recovery and documentation. [Examples: Backup processes, mirroring hard drives (RAID method), uninterrupted power supply, separate storage, virus protection/firewall, emergency plan.]*

* 1. Separation control

*Are the data of the principal being processed separately from other customers’ data? Are the data being processing in development or test environments and if so how? [Examples: separation of functions.]*

**APPENDIX 3**

**Local Law Amendments**

Data Exporter remains the appropriate contact person for the data subject, i.e. Data Exporter, in addition to Data Importer, remains responsible for data subject’s right to information, deletion, corrections, blocking and damages.

**ANNEX B**

**DESCRIPTION OF THE TRANSFER**

**Data Exporter**

The data exporter is:

* *[IU Consulting and Research Germany GmbH]*

**Data Importer**

The data importer is:

* *[Indiana University]*

**Data Subjects**

The personal data transferred concern the following categories of data subjects: [….]

**Purposes of Transfer**

The transfer is made for the following purposes:

* [….]

**Categories of Data**

The personal data transferred concern the following categories of data:

* […]

**Recipients**

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

* […]

**Sensitive Data (**if appropriate)

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

*Sensitive data will not be tracked or processed.*

**Additional Useful Information** (storage limits and other relevant information)

The personal data transferred may be stored for *[…months/years or criteria for determining storage period]*

**SIGNATURE**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Place/date Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Place/date Name