Data Transfer Agreement
(controller to controller),
dated _____, 20__

[name of the counterparty], established and existing in accordance with the legislation of [name of the country], represented by [job title and full name of the authorized person], acting under [the basis of authority], hereinafter referred to as the "Controller" or "the data exporter", on the one hand, and

[name of the counterparty], established and existing in accordance with the legislation of [name of the country], represented by [job title and full name of the authorized person], acting under [the basis of authority], hereinafter referred to as the separate "Controller" or "the data importer" on the other hand, and jointly referred to as the "Parties", have entered into this Data Transfer Agreement as follows.

1. **General provisions**

Based on Article 32(4) of the General Data Protection Regulation of April 27, 2016 (EC) 2016/679 ("GDPR"), the controller shall take steps to ensure that any natural person acting under the authority of the controller who has access to personal data does not process them except on instructions from the controller, unless he / she is required to do so by Union or Member State law.

2. **Terms and definitions**

The following terms and definitions shall be used for the purposes of this Data Transfer Agreement:
Personal data processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Personal data processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Controller – a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Personal data transfer – any act of transmitting personal data by any means (including physical and electronic ones), providing access to personal data, including remote access and saving, inserting personal data in the information system(s).

3. **Information about personal data processing**

3.1 Categories of data subjects whose personal data is transferred:
[list of categories of data subjects].
3.2 The purposes of personal data processing are:
- [list PD processing purposes].

3.3 List of categories of personal data processed:
- [list categories of personal data].

3.4 The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:
- [duration of personal data processing].

3.5 The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis.

4. Rights and responsibilities of the Parties

4.1. Each of the Parties is independently acting as a controller of personal data with respect to personal data transferred to it by the other Party. The other should be directly specified in the agreement on the assignment of personal data processing, if such agreement is concluded between the Parties in respect of certain cases of personal data processing.

4.2. The data exporter, on the basis of the respective inquiry received from the data importer, shall confirm to the data importerthat it has obtained consents of personal data subjects for transfer of their personal data, or that the data exporter has other legal grounds for the personal data transfer and it has duly notified the subjects about transfer of their personal data.

4.3. The Parties shall maintain confidentiality and security of the transferred to each other personal data during their processing in accordance with requirements of the applicable national legislation of [name of the country] and [name of the country] and Section 5.

4.4. The data importer has the right to transfer to third parties the personal data received from the data exporter for the purposes provided for in this Data Transfer Agreement in the presence of relevant legal grounds for such transfer and on condition that mentioned third parties shall maintain confidentiality and security of personal data during their processing. The data importer shall upon request of the data exporter to provide information about third parties engaged to personal data processing, as well as information about which personal data, what subjects and for what purpose were transferred to third parties.

4.5. Each Party shall compensate the other Party for any losses caused to the injured Party as a result of unlawful transfer of personal data from the guilty Party to the injured Party or breach of personal data confidentiality and (or) security that occurred through the fault of the guilty Party during processing of personal data received from the injured Party. Such losses will be compensated in the amount of documented real damage.

4.6. The data importer undertakes immediately inform the data exporter about the received requests (claims, demands) of:

- data subject (data subject's representative) with regard to processing and (or) protection of his / her personal data, received by data importer in the framework of this Data Transfer Agreement;
- authorized body with regard to processing and (or) protection of personal data, received by data importer in the framework of this Data Transfer Agreement;
- other party with regard to processing and (or) protection of personal data, received by data importer in the framework of this Data Transfer Agreement.

4.7. The Parties hereby agree to cooperate in good faith and provide the necessary assistance to each other in the settlement of requests (claims, demands) received by either Party from personal data subjects, authorized bodies or other parties in connection with alleged violations of the requirements of applicable law regarding the processing and (or) protection of personal data transferred between the Parties.

5. Data protection safeguards

5.1. The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

5.2. The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in clause 3.2. B. It may only process the personal data for another purpose:

- where it has obtained the data subject's prior consent;
- where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

- where necessary in order to protect the vital interests of the data subject or of another natural person.

5.3. Transparency

a) In order to enable data subjects to effectively exercise their rights pursuant to Article 12-22 of GDPR, the data importer shall inform them, either directly or through the data exporter:
   - of its identity and contact details;
   - of the categories of personal data processed;
   - of the right to obtain a copy of these Clauses;
   - where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground.

b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of GDPR.

5.4. Accuracy and data minimisation

a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

5.5. Storage limitation

a) The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation[1] of the data and all back-ups at the end of the retention period.

5.6. Security of processing

a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

[1] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible

b) The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.
e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.
f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.
g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

5.7. Sensitive data

a) Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

a) Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

5.8. Processing under the authority of the data importer

a) The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

5.9. Documentation and compliance

a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

b) The data importer shall make such documentation available to the competent supervisory authority on request.

6. **Other provisions**

6.1. The Data Transfer Agreement shall enter into force when signed by both Parties and remain in force without limit of time. This Agreement can be terminated by mutual agreement of the Parties.

Signatures of the Parties

Party 1

[Name of the Controller]

[Address of the Controller]

_____

[Position of authorized person] / [Full name]

Party 2

[Name of the Controller]

[Address of the Controller]

_____

[Position of authorized person] / [Full name]