Terms and Conditions for Data Collection

1. *Introduction*

Data submitted by the providing party are available for conducting business discussion and collaboration on related IT solution consultations. Their provision is subject to conditions and is carried out according to an established procedure.

The providing party only submit information and data that are necessary to the specific question on related IT solutions. The information and data to be provided is purely use for the enquiry of specific questions.

Upon data provision, the data are supplied to the receiving party on a one-time basis under the established in this input form and further IT solution consultations and subsequent business collaboration. The receiving party may not distribute, deliver, or share the provided data with any third party. Furthermore, the receiving party is not using the provided data internally for other purposes.

The providing party confirms that, where applicable, informed consent has been obtained from each individual, organization, limited company, and similar in accordance with applicable law. This consent explicitly includes the transfer of the data for the intended purpose.

The providing party commits solely to supplying the data to the receiving party. No warranty is given that these data are (fully) suitable for the receiving party's intended purposes.

2. *Confidentiality*

The providing party, the receiving party, and any individuals they engage in the business collaboration are obliged to maintain strict confidentiality regarding all information and data they encounter in the context of such business collaboration. The receiving party declares that all discussions and information exchanged will be kept strictly confidential and that it will not use or misuse such information for its own or any third party's benefit.

The data may only be used for the agreed purposes and may not be shared with third parties. Notwithstanding the foregoing, the receiving party is permitted to discuss or provide the data to third parties only after obtaining written consent from the providing party. The providing party may condition such consent on the third party entering into a confidentiality agreement with it.

3. *Ownership*

The providing party is not obliged to disclose any specific data and retains all rights to the data at all times.

The receiving party shall not remove or alter anything in or about the data without the explicit consent of the providing party.

All existing intellectual property rights and data shared under the Data Provision Agreement remain the property of the providing party. Any new intellectual property rights or data developed jointly that do not belong exclusively to one organization shall be jointly owned by the providing party and the receiving party.

4. Obligation to delete data

The receiving party commits to delete all (digital) documents and data provided by or on behalf of the providing party, including all (digital) copies, upon the first request of the providing party. The receiving party may not retain any copies or provide the data to third parties.

The receiving party is not entitled to invoke any potential authority and/or right to withhold the data, such as a possible right of suspension. The receiving party expressly waives any right to rely on such authorities or rights.

5. Violation relating to personal data

The receiving party shall inform the providing party as soon as possible, and no later than 24 hours, after a (suspected) personal data breach has been identified. To the extent known, the report shall include the cause of the breach, the category of personal data, the individuals affected, and the number of individuals involved.

In the event of a breach, the receiving party shall immediately take all necessary actions to remediate the breach, mitigate its consequences, and prevent further breaches.

6. Security

The receiving party shall take appropriate technical and organizational measures to protect the data against loss or unlawful processing. These measures shall ensure an adequate level of security, taking into account the state of the art, implementation costs, the risks associated with processing, and the nature of the data to be protected. The data may only be stored on devices owned by the receiving party.

The receiving party shall immediately inform the providing party of any security breach involving the provided data. The providing party shall have the right to review the technical and organizational measures the receiving party has implemented to protect the data.