Data Processing Agreement

Between Industrie Reply GmbH (hereinafter: “Supplier”), and the contracting person or entity indicated in the **AXULUS** Order Form (hereinafter: “Client”); jointly referred to as the “Parties”, whereas

a) An agreement has been entered into between the Supplier and the Client (hereinafter: “Main Agreement”) concerning the Client’s right to use the **AXULUS** Suite and the provision, by the Supplier, of remote assistance services, relating to use of the AXULUS Suite (hereinafter: “Services”)
b) For the purposes of this Data Processing Agreement, the terms “Data Controller”, “Data Processor”, “data subject”, “processing”, “Supervisory Authority” shall have the meaning ascribed to such terms in the GDPR.

Now, therefore, (the recitals to be considered as an integral and substantial part of the deed of appointment), the Parties hereby agree as follows.

1. Subject matter, term of the order, type and the purpose of the processing, type of personal data, categories of data subjects

The subject matter and the term of the order, the type and the purpose of the processing, the type of personal data and the categories of the data subjects result from the main agreement between the parties. The order ends upon the expiration of the main agreement. If no provisions are stipulated in the main agreement in respect of the aforementioned regulation, Annex 1 to this agreement shall apply.

2. Security of processing
In its area of responsibility, the supplier shall meet the agreed technical and organisational measures pursuant to Art. 5(1) and Art. 32 GDPR (General Data Protection Regulation) and shall structure its internal business organisation in line with data protection law requirements. This encompasses the technical and organisational measures set out in Annex 2.

3. Correction, erase and restriction of data
The supplier shall not correct or erase or restrict the processing of data processed to order, unless upon the customer’s instruction. If a data subject contacts the supplier directly for the correction or erasure of his/her data or the restriction of the processing, the supplier shall pass on such request to the customer without delay.

In the event of assertion of legal rights of a data subject, the supplier shall support the customer; this comprises, but is not limited to the support in answering applications for the safeguarding of rights of a data subject by way of appropriate technical and/or organisational measures.

4. Obligations of the supplier
The supplier shall ensure the compliance with the following duties:

a) Written appointment - to the extent as legally required - of a data protection officer.
If the person acting as data protection officer is replaced, the customer shall be informed thereof without delay.

b) All persons allowed to access personal data of the customer in accordance with the order must be bound to confidentiality in writing and informed of the special data protection duties resulting from this order as well as the existing commitment to instructions and to a specific purpose. On the customer’s request, the supplier shall submit the declarations of commitment to the customer. This will not be necessary if the relevant persons are subject to a reasonable statutory obligation of non-disclosure.

c) Toleration of public audits by the appropriate data protection supervisory authorities to the same extent as the data protection supervisory authorities are allowed to conduct audits with the customer. Support of the customer in connection with the audits and inquiries of the supervisory authorities.

d) Immediate information of the customer about audit actions and measures of the supervisory authority. This also applies if an appropriate authority conducts investigations against the Supplier pursuant to Art. 82 et seq. GDPR.

e) Reasonable support to the Customer in connection with the guarantee of processing security pursuant to Art. 32 GDPR.

f) Reasonable support to the customer in connection with data protection impact assessments pursuant to Art. 35 GDPR and the prior consultation of the appropriate data protection supervisory authorities pursuant to Art. 36 GDPR.

g) Reasonable support to the customer in connection with the reporting of breaches of the protection of personal data to the supervisory authority (Art. 33 GDPR) and the information of the persons affected by breaches of the protection of personal data (Art. 34 GDPR).

h) The delivery of the information required by Art. 30(2) GDPR.

5. Subcontracts
a) In relation to the foregoing, the Client hereby authorizes the Supplier to appoint its own Sub Data Processors. A current list of Data Subprocessors by Supplier is available at www.axulus.io.

b) For the awarding of a subcontract, the supplier shall design the contractual arrangements between the supplier and the subcontractor in such a manner as to align them to the data protection and data safety requirements between the parties to this agreement. Where the subcontractor fails to fulfil its data protection obligations, the supplier shall remain fully liable to the customer for the performance of the subcontractor’s obligations. In the event of proven justified interests, the customer may object to subcontracting. On the customer’s written request, the supplier shall provide information to the customer about the essential contents of the contract (services, without prices) and the implementation of the subcontractor’s duties with data protection relevance.

c) The supplier always informs the customer of the processor shall inform the controller of any intended changes concerning the addition or replacement of subcontractors, thereby giving the customer the opportunity to object to such changes.

6. Place of procession
The processing of the data by the supplier is limited to the territory of the EU and the EEA. The transfer of data by the supplier to a recipient resident outside the EEA is only permitted subject to the conditions of Art. 44 et seq. GDPR and requires the separate prior written consent of the Customer. The Supplier shall particularly ensure that the customer will be able to agree on the standard contractual clauses (cf. e.g. the decision of the European Commission of 5 February 2010, published in the Official Journal of the European Union L39/5, C (2010) 593) with the data recipient.

7. Control rights of the customers
Upon timely written notification, the customer may satisfy itself of the reasonable nature of the measures for the compliance with the technical and organisational requirements of the data protection laws applicable to order processing and may do so for inspection purposes on the business premises within the usual business hours without disturbing the business routine. The supplier shall tolerate the inspections of the customer under this agreement, provide collaboration services to the extent as required for the customer’s inspection under this agreement, and give information to the customer on its written request within a reasonable period, which are required for conducting a comprehensive order control. The supplier shall particularly enable the customer to satisfy itself of the compliance with the technical and organisational measures taken by the supplier prior to the commencement of data processing and then on a regular basis.

8. Notifications of data breaches and processing errors

In each case, the supplier shall inform the customer immediately upon getting knowledge that the supplier, any of the individuals employed by the supplier or the subcontractors it uses violated the regulations on the protection of the customer's data (particularly the GDPR) or the stipulations set forth in this agreement or if there is any suspicion in this respect. The supplier shall document such events, clarify them without delay and initiate corrective action. The supplier shall keep the customer informed of the progress of the matter until the remediation of the event. If the violation should entail a risk to the rights and freedoms of the data subjects as defined in Art. 33 GDPR, the supplier shall provide comprehensive support to the customer for the clarification of the event and in connection with the corresponding report to the data protection supervisory authority or the data subject, respectively.

9. Instructions of the customer

The handling of the data shall be in accordance with the agreements made and the customer's instruction on an exclusive basis. Within the framework of the order specification set forth in this agreement, the customer reserves a comprehensive power to give instructions relating to the type, scope and method of the data processing, which the customer may specify in more detail by way of individual instructions. Changes of the subject matter of processing and changes of methods shall be coordinated jointly and documented. The supplier shall not give any information to third parties or the data subject, unless with the prior written consent of the customer. Following oral instructions, the customer will confirm such instructions immediately in writing or via email (in text form as defined in the German Civil Code).

The supplier shall not use the data for any other purposes and is particularly not entitled to pass them on to any third party. Copies and duplicates shall not be prepared without the customer's knowledge. Backup copies are excluded from the foregoing to the extent they are needed to ensure proper data processing; likewise, data are excluded which are required in the context of compliance with statutory retention periods. The supplier shall inform the customer immediately if the supplier is of the opinion that an instruction would violate data protection regulations. The supplier has the right to suspend the implementation of the respective instruction until confirmed or changed by the responsible person within the customer's organisation. The supplier shall document the instructions as required.

10. Return and erase of data

Upon the end of the agreement and subject to agreements providing otherwise and duties provided by law or the articles of association, the supplier shall immediately return to the customer the data media provided to the supplier and to erase personal data the supplier received in connection with the order, which have not been erased before. The customer shall decide on return or erasure upon the end of the agreement within a period set by the supplier. If the supplier does not return to the customer documents or data media with personal data subject to erasure, the supplier shall dispose of the documents in a proper manner, concurrently preventing that third parties could get knowledge of the data. If the supplier incurs costs due to the return or erasure of the customer's data after the end of the agreement, the customer shall bear such costs.

ANNNEX 1: SPECIFICATIONS

Specifications Required under Data Protection Law

Subjectmatter of processing

Scaling Industry Internet of Things Solutions

Duration of processing

According to the Main Agreement

Scope, type and purpose of the envisaged collection

• Cloud based subscription by the Client • Deployment in the company's Azure Tenant • The Client chooses the Scope according to the selected templates

Type of personal data

Account information, eg. username, password
Log files

Categories of data subjects

Client's Employees
Client's Customers
Client's Suppliers

ANNEX 2: SECURITY MEASURES

Depending on the activities performed, insofar as applicable to the purpose of the agreement, the following security measures shall be implemented by the Data Processor and by any sub-data processors, if authorised.

- Asset management: if the service offered by the Supplier includes the management of IT assets, an inventory of the assets used for processing information needs to be defined and maintained, together with a list of the type of information processed.

- Procedures for the secure erasure of the data processed on behalf of the Client (e.g. demagnetization or physical destruction) shall be agreed upon with the Data Controller at the end of the collaboration and in any case in the event of reuse, disposal or transfer to third parties of electronic tools or storage media. Safe deletion methods are also used for paper documentation.

- Physical security: appropriate security measures shall be taken if activities are performed on behalf of the Client at the Supplier's premises.

- Logical access control: correct user access methods shall be established in order to prevent any unauthorized processing of information. If as part of the activities it carries out, the Supplier needs to access the Client's resources, the Supplier shall comply with the authorization procedures defined by the Client. If as part of the service, the Supplier is authorized to independently manage the users:
  - Access to information shall be restricted by implementing technical and organisational controls.
  - Access to information and resources shall be restricted, according to the "need to know[1]", "least privilege[2]" and "separation of duties[3]" principles, where possible.

    In order to access the information contained in the systems, a user identification and authentication process shall be activated and relevant authorizations shall be activated in compliance with the principles mentioned in the previous point.

    System administrator users with special privileges shall be handled with special care and in compliance with relevant provisions of law.

    A user management process shall be defined and documented which includes all credential lifecycle phases, from creation to deactivation.

    Password management methods shall be introduced with password change and password complexity mechanisms. Passwords shall be stored and transmitted using secure methods.

    Infrastructure systems shall be suitably protected and segregated, where possible, to minimize the chances of unauthorized logical access. Special attention is given to systems having connections with the outside world.

- Operating management of systems, networks and telecommunications: as part of the IT system management activities carried out on behalf of the Client, where contractually provided for, an appropriate IT system security level shall be reached during operation in order to adequately protect the information being processed.
  - Appropriate measures to prevent and identify any potentially harmful software (e.g. viruses, malware, …) shall be implemented
  - Plans and procedures shall be defined in order to manage operating system, software and data backups, where such activity is envisaged
  - The patches released for the systems used shall be constantly monitored; new security assessment methods shall be defined and, if necessary, implemented.
  - The network shall be appropriately designed to ensure data protection. The information systems used and managed during the activities performed for the Client offer perimeter security to protect against any unauthorized access.

- Development, maintenance and acquisition of IT systems: IT systems (applications, operating systems, middleware, etc.) shall be developed or purchased and maintained over time to safeguard information confidentiality, integrity and availability

  If the activities performed by the Supplier regard design and development activities, security requirements are appropriately considered, implemented and checked, *inter alia* in accordance with the "by design/by default" privacy principle.

- Security measures for sub-contracting If authorized by the Client, activities shall be sub-contracted by correctly determining and implementing the security requirements regulating the respective business relationships.

- Security incident management – Incidents shall be detected immediately and reported to the Client; if applicable, any damages shall be dealt with as quickly as possible, *inter alia* according to the Data Breach Notification process.

[1] The *need to know* principle requires that access rights to information are in line with and not exceed the position held in the company; information that is not useful for correctly and efficiently performing job duties may not be seen

[2] The *least privilege* principle requires that access privileges do not exceed the position held in the company (e.g. if for a given function, data may be simply consulted, access rights allowing the data's modification shall not be given).

[3] *Separation of duties* requires that the same person is not responsible for authorizing and performing an action.