Agreement

between business customers

- hereinafter referred to as "Controller" -

and Uniscon GmbH

- hereinafter referred to as "Processor"

concerning the use of the service idgard

Preamble

The Controller intends to commission the Processor, among other things, with the processing of personal data of the Controller within the scope of the performance of concluded and/or still to be concluded individual contracts. The purpose of this agreement is to set out the data protection framework conditions and the obligations of the contracting parties in this respect, which shall continue to apply unchanged in the course of the future commissioning. This agreement shall apply to all activities which are connected with the fulfillment of the respective individual contract and during which employees of the Processor or third parties commissioned by the Processor come or may come into contact with personal data of the Controller. This agreement shall be supplemented by specific, order-related data protection regulations, which shall be agreed in each case in a corresponding individual contract referring to this order.

A special feature of the idgard service is that so-called "operator security" is provided by the Processor. The structure of the systems is designed according to the principle of "Sealed Cloud", which means that even if all the technical-organizational measures mentioned in this agreement are circumvented, no access to the data in the electronically, cryptographically and mechanically sealed data center can be made by proportionate means. Details on the principle of the Sealed Cloud are published on the website www.idgard.de.

The protection by sealing by means of Sealed Cloud concerns the personal data arising in connection with the use of idgard, including the username, the password, and the "Password Unblocking Key" (PUK) of the Administrator, but with the exception of the data collected during registration by the Processor and required for billing the service (e.g. number of licenses). For all data, however, at least the technical-organizational measures specified in this Agreement shall apply.

Also included in the special protection of the Sealed Cloud is the data required to restore user access to idgard in the event of a lost username or password and PUK of the administrator at the Controller. For this purpose, idgard offers so-called trustee boxes.

This agreement is only necessary if one follows the legal theory of the so-called absolute or objective personal reference of data. If one follows the legal theory of the so-called relative or subjective personal reference, this agreement is not necessary, as the data protected by the Sealed Cloud is not personally identifiable for the Processor.

The following agreement is therefore concluded purely as a precautionary measure.

1. Subject and duration of the order

The subject and duration of an order is specified in the respective individual contract.

2. Specification of the agreement details

(1) The scope, nature and purpose of the processing as well as the type of data and the group of data subjects are likewise described in the respective individual contract. Notwithstanding the foregoing, the Processor shall be entitled to carry out all necessary processing steps and uses of the data provided by the Controller and of the data collected for the Controller (e.g. duplication of inventories for loss protection, creation of log files, intermediate files and work areas, etc.) in order to fulfill the respective subject matter of the contract in compliance with the provisions of this Agreement and the provisions of the respective individual contract, insofar as this does not lead to a transformation of the content.

(2) The processing and use of the data takes place exclusively in the territory of the Federal Republic of Germany.

3. Technical-organizational Measures

(1) The Processor shall document the implementation of the technical and organizational measures set out and required prior to the award of the contract before the start of the processing, in particular with regard to the specific execution of the contract, and shall hand them over to the Controller for inspection. If accepted by the Controller, the documented measures shall become the basis of the order. Insofar as the examination/audit of the Controller reveals a need for adaptation, this shall be implemented by mutual agreement.

(2) The Processor shall establish security pursuant to Article 28(3), point (c) and Article 32 of the GDPR, in particular in connection with Article 5(1-2) of the GDPR. Overall, the measures to be taken are data security measures and to ensure a level of protection appropriate to the risk with regard to confidentiality, integrity, availability and the resilience of the systems. In this context, the state of the art, the implementation costs and the nature, scope and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32(1) of the GDPR shall be taken into account. Details are set out in the respective current Annex 1 (TOM).

(3) The technical and organizational measures are subject to technical progress and further development. In this respect, the Processor is permitted to implement alternative adequate measures. In doing so, the security level of the specified measures must not be undercut. Significant changes shall be documented.

4. Correction, restriction and deletion of data

(1) The Processor may not correct, delete or restrict the processing of data processed autonomously, but only in accordance with documented instructions from the Controller. Insofar as a data subject contacts the Processor directly in this regard, the Processor shall forward this request to the Controller without delay.

(2) Insofar as included in the scope of services, the deletion concept, right to be forgotten, correction, data portability and access shall be ensured directly by the Processor in accordance with the Controller's documented instructions.

5. Quality assurance and other obligations of the Processor

(1) In addition to compliance with the provisions of this agreement, the Processor has statutory obligations pursuant to Articles 28 to 33 of the GDPR; in this respect,

the Processor shall in particular ensure compliance with the following requirements:

a. Written appointment of a data protection officer who performs his activities in accordance with Articles 38 and 39 GDPR. The contact details of the data protection officer shall be communicated to the Controller for the purpose of direct contact upon request. The Controller shall be informed immediately of any change of data protection officer.

b. The maintenance of confidentiality pursuant to Article 28(3), sentence 2, point b; Article 29 and Article 32(4) of the GDPR. When carrying out the work, the Processor shall only use employees who have been obligated to maintain confidentiality and who have previously been familiarized with the data protection provisions relevant to them. The Processor and any person subordinate to the Processor who has access to personal data may process this data exclusively in accordance with the Controller's instructions, including the powers granted in this Agreement, unless they are legally obligated to process it.

c. The implementation of and compliance with all technical and organizational measures required for this order in accordance with Article 28(3), point c, and Article 32 of the GDPR as per Annex 1.

d. The Controller and the Processor shall, upon request, cooperate with the Supervisory Authority in the performance of its duties.

e. The immediate information of the Controller about control actions and measures of the supervisory authority, insofar as they relate to this agreement. This shall also apply insofar as a competent authority investigates in the context of administrative offense or criminal proceedings with regard to the processing of personal data during the commissioned processing at the Processor.

f. Insofar as the Controller is exposed to an inspection by the supervisory authority, administrative offense or criminal proceedings, a liability claim by a data subject or a third party or any other claim in connection with the commissioned processing at the Processor, the Processor shall support the Controller to the best of its ability.

g. The Processor shall regularly monitor the internal processes as well as the technical and organizational measures to ensure that the processing in its area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the protection of the rights of the data subject is ensured.

h. Verifiability of the technical and organizational measures taken vis-à-vis the Controller within the scope of its control powers pursuant to Section 7 of this Agreement.

6. Subcontracting

(1) Subcontracting relationships within the meaning of this provision shall be understood to be those services which relate directly to the provision of the main service. This does not include ancillary services which the Processor uses, for example, as telecommunications services, postal/transport services, maintenance and user service or the disposal of data carriers and other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the Processor shall be obligated to implement appropriate and legally compliant contractual agreements as well as control measures to ensure data protection and data security of the Controller's data even in the case of outsourced ancillary services.

(2) The Processor may only engage subprocessors (further Processors) with the prior express written or documented consent of the Controller. The outsourcing to subprocessors or the change of the existing subprocessor are permissible insofar as (i) the Processor notifies the Controller of such outsourcing to subprocessors in writing or in text form a reasonable time in advance and (ii) the Controller does not object to the planned outsourcing to the Processor in writing or in text form by the time of the transfer of the data and (iii) a contractual agreement in accordance with Article 28 (2-4) of the GDPR is used as a basis.

7. Inspection rights of the Controller

(1) The Controller shall have the right to carry out inspections in consultation with the Processor or to have them carried out by inspectors to be named in individual cases. It shall have the right to satisfy itself of the Processor's compliance with this Agreement in its business operations by means of random checks, which must generally be notified in good time.

(2) The Processor shall ensure that the Controller can satisfy itself of the Processor's compliance with its obligations pursuant to Article 28 of the GDPR. The Processor undertakes to provide the Controller with the necessary information upon request and, in particular, to provide evidence of the implementation of the technical and organizational measures.

(3) Evidence of such measures, which do not only relate to the specific order, can be provided by current test certificates, reports or report extracts from independent bodies (e.g. auditors, auditing, data protection officers, IT security department, data protection auditors, quality auditors); or suitable certification by IT security or data protection audit (e.g. in accordance with *BSI-Grundschutz*, the basic protection by the German Federal Office for Information Security).

(4) The Processor may claim remuneration for enabling inspections by the Controller.

8. Notification of violations by the Processor

(1) The Processor shall support the Controller in complying with the obligations set out in Articles 32 to 36 of the GDPR regarding the security of personal data, data breach notification obligations, data protection impact assessments and prior consultations. This includes, among other things

- Ensuring an adequate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing, as well as the predicted likelihood and severity of a potential security breach, and allow for the immediate detection of relevant breach events
- The obligation to report personal data breaches to the Controller without delay
- the obligation to assist the Controller within the scope of its duty to inform the data subject and, in this context, to provide it with all relevant information without delay
- the support of the Controller for its data protection impact assessment
- support of the Controller within the framework of prior consultations with the supervisory authority

(2) The Processor may claim compensation for support services that are not included in the Statement of Work or are not due to the Processor's misconduct.

(3) A liability provision agreed between the parties in the individual contract shall also apply to commissioned processing, subject to an express agreement to the contrary.

9. Authority of the Processor to issue instructions

(1) The Controller shall confirm verbal instructions without delay (at least in text form).

(2) The Processor shall inform the Controller immediately if it is of the opinion that an instruction violates data protection regulations. The Processor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Controller.

10. Deletion and return of personal data

(1) Copies or duplicates of the data will not be made without the knowledge of the Controller. Excluded from this are security copies, insofar as they are necessary to ensure proper data processing, as well as data that is required with regard to compliance with statutory retention obligations.

(2) After completion of the contractually agreed work or earlier upon request by the Controller - at the latest upon termination of the service agreement - the Processor shall hand over to the Controller all documents, processing and utilization results created and data files related to the contractual relationship that have come into its possession or, after prior consent, destroy them in accordance with data protection requirements. The same shall apply to test and reject material. The protocol of the deletion shall be submitted upon request.

(3) Documentation that serves as proof of orderly and proper data processing shall be kept by the Processor beyond the end of the contract in accordance with the respective retention periods. The Processor may hand them over to the Controller at the end of the contract to relieve the Processor.

The above is a convenience translation. In case of doubt or contradiction, the German language version shall prevail.

Appendix 1: Technical and organizational measures

Company of the Controller

Street, house number, postal code and city of the Controller

Signature business Controller (Controller)

(Place, date, signature)

Signature Uniscon GmbH (Processor)

(Place, date, signature)

Please sign and return duplicate copies of this agreement to:

uniscon universal identity control GmbH
Ridlerstrasse 57 | Newton
80339 Munich