Appendix C:

Instructions on the use of personal data

1. The subject of/instruction for the processing

The Data Processor's processing of personal data on behalf of the Data Controller shall be carried out by the Data Processor performing the following:

- Personal data is processed for the purpose of providing the Services to Users.

2. Security of processing

The level of security that shall be taken into account: Processing involves a large volume of personal data which is why a "high" level of security should be established.

The Data Processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The Data Processor shall, however– in any event, and at a minimum– implement the following measures that have been agreed with the Data Controller:

2.1. Information security policies. A set of policies for information security is defined, approved by management, published, and communicated to employees and relevant external parties.

2.2. Organisation of information security. Information security responsibilities are defined and allocated.

2.3. Human resource security. Background verification checks are carried out in accordance with relevant laws and regulations and contractual agreements state the responsibilities for information security. All team members receive appropriate awareness education and regular updates in organisational policies.

2.4. Asset management. An inventory of information assets and processing facilities is maintained and rules for acceptable use are documented and implemented. Information is classified and procedures for the handling of assets in accordance with the classification scheme are implemented.

2.5. Access control. An access control policy is established, documented, and reviewed and access to information and applications is restricted accordingly. Processes for user registration and deregistration as well as access provisioning are implemented. Access rights are reviewed at regular intervals.

2.6. Cryptography. A policy on the use of cryptographic controls for the protection of information is implemented.

2.7. Physical security. Systems are exclusively hosted in data centres providing adequate standards for information security.

2.8. Operations security. Operating procedures are documented and changes to information processing facilities are controlled. Development, testing, and operational environments are separated to reduce the risk of unauthorised changes to the operational environment. Controls to protect against malware are implemented and backups of information are taken and tested regularly. Event logs recording system administrator activities and security events are produced and regularly reviewed. Information about technical vulnerabilities of information systems is obtained in a timely fashion and appropriate measures to address the associated risk are taken.

2.9. Communications security. Networks are managed and controlled to protect information and groups of information services are segregated on networks. Communication with applications utilised cryptographic controls such as TLS to protect the information in transit over public networks. Stateful firewalls, web application firewalls, and DDoS protection are used to prevent attacks.

2.10. System acquisition, development, and maintenance. Information security requirements are taken into consideration for new information systems or enhancements to existing information systems. Rules for the secure development of software and systems are established and applied and testing of security functionality is carried out in regular intervals.

2.11. Incident management. Incident management responsibilities and procedures are established to ensure quick, effective, and orderly response to security incidents.

3. Assistance to the Data Controller

The Data Processor shall insofar as this is possible assist the Data Controller by implementing the following technical and organisational measures:

3.1. Measures for ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services

3.2. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

3.3. Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures to ensure the security of the processing

3.4. Measures for User identification and authorization

3.5. Measures for the protection of data during transmission

3.6. Measures for the protection of data during storage

3.7. Measures for ensuring the physical security of locations at which personal data are processed

3.8. Measures for ensuring events logging

3.9. Measures for internal IT and IT security governance and management

3.10. Measures for certification/assurance of processes and products

3.11. Measures for ensuring data minimization

3.12. Measures for ensuring data quality

3.13. Measures for ensuring limited data retention

3.14. Measures for ensuring accountability

3.15. Measures for allowing data portability and ensuring erasure

4. Storage period/erasure procedures

Personal data is stored for the time of providing the Services to Users after which the personal data is automatically erased by the Data Processor.

Upon termination of the provision of personal data processing services, the Data Processor shall either delete or return the personal data in accordance with Clause 10.1., unless the Data Controller – after the signature of the contract – has modified the Data Controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the Data Controller's prior written authorisation:

- Europe
- United States

European OEM customers can choose a configuration (by excluding the optional components listed in Appendix B) where all personal data processing is performed exclusively in European locations.

6. Instruction on the transfer of personal data to third countries

As recommended by the European Data Protection Board (EDPB), when personal data is transferred to third countries, appropriate transfer tools are verified in accordance with Chapter V GDPR (the transfer tools listed under Articles 46 GDPR). Additionally, the law or practice of the third country is assessed, and supplementary measures are identified and adopted to bring the level of protection of the data transferred up to the EU standard of essential equivalence. The level of protection is reevaluated at appropriate intervals.

If the Data Controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the Data Processor shall not be entitled within the framework of the Clauses to perform such transfer.

7. Procedures for the Data Controller's audits, including inspections, of the processing of personal data being performed by the Data Processor

As required pursuant to article 28(3)(h) GDPR, the Data Processor will allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller required pursuant to article 28(3)(h) GDPR. The Data Controller shall give the Data Processor reasonable notice of any audit or inspection to be conducted and shall make (and ensure that each of its mandated auditors makes) reasonable effort to avoid any damage, injury or disruption to the Data Processor, its premises, equipment, personnel and business. Under all circumstances, all costs concerning an audit are borne by the Data Controller.

Signature Certificate

Reference number: W6XJJ-WOGAY-TYSLD-7ZRMV

Signer	Timestamp	Signature
Robert Strobl Email: rs@digitalsamba.com		
Sent:	15 Nov 2022 08:04:16 UTC	
Viewed:	15 Nov 2022 08:04:36 UTC	
Signed:	15 Nov 2022 08:04:52 UTC	
Recipient Verification:		IP address: 84.115.213.183
✔Email verified	15 Nov 2022 08:04:36 UTC	Location: Vienna, Austria
Denis Agca Email: denis@vulcavo.de		
Sent:	15 Nov 2022 08:04:16 UTC	
Viewed:	06 Jan 2023 09:05:51 UTC	
Signed:	06 Jan 2023 09:07:56 UTC	
Recipient Verification:		IP address: 91.46.138.224
✔Email verified	06 Jan 2023 09:05:51 UTC	Location: Bergisch Gladbach, Germany

Document completed by all parties on:

06 Jan 2023 09:07:56 UTC