DATA PROCESSING AGREEMENT

("**Agreement**")

between

Registered Symphony Users
("**CONTROLLER**")

and

COMMEND International GMBH
Saalachstrasse 51
5020 Salzburg
AUSTRIA
("**PROCESSOR**")

as follows:

1. SUBJECT MATTER, NATURE AND PURPOSE OF THE PROCESSING

1.1. PROCESSOR operates a cloud-based communication solution focusing on applications for security, safety and productivity that is available through a web interface as well as a mobile application (Symphony).

1.2. CONTROLLER uses the Symphony system for its own purposes.

1.3. PROCESSOR processes personal data of the data subjects as referred to in Section 2 of Annex 1 (“data subjects”) on behalf of the CONTROLLER in the scope of the activities according to Annex 1 (Section 1) of this Agreement. This processing will be performed on the basis of the underlying contract between PROCESSOR and CONTROLLER ("Main Contract"). Other data, especially functions that were collected and not defined by the corresponding Main Contract, or data processed in a different manner are explicitly not included in the instruction of the CONTROLLER.

2. DURATION OF THE PROCESSING

2.1. PROCESSOR uses the personal data according to the instructions of CONTROLLER only as long as:

- the relevant underlying contract is not terminated or expired and the processing is necessary for the completion of the activities described and instructed in Annex 1 (Section 1) of this Agreement,

- this Agreement has not been terminated according to Section 7.1., or
- the authorization to process personal data according to this Agreement or its part was not withdrawn by the CONTROLLER.

2.2. Further conditions for the processing according to this Agreement, especially the processing purpose as determined by the CONTROLLER, the categories of personal data and the categories of the data subjects are defined in Annex 1 to this Agreement.

3. RIGHTS AND OBLIGATIONS OF THE CONTROLLER

3.1. CONTROLLER is in the position of a data controller in the meaning of Art 4 ciph 7 GDPR with respect to any kind of information according to Annex 1 to this Agreement relating to the identified or identifiable persons as defined in Art 4 ciph 1 GDPR ("personal data") and committed to PROCESSOR acting as data processor according to Art 4 ciph 8 GDPR in the course of the activities according to Annex 1 (Section 1) of this Agreement.

3.2. CONTROLLER has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3.3. CONTROLLER shall be responsible, amongst others, for ensuring that the processing of personal data, which the PROCESSOR is instructed to perform, has a legal basis.

4. RIGHTS AND OBLIGATIONS OF THE PROCESSOR

4.1. General

4.1.1. PROCESSOR is in a position of a processor in the meaning of Art 4 ciph 8 GDPR with respect to any kind of information according to Annex 1 to this Agreement relating to the identified or identifiable persons as defined in Art 4 ciph 1 GDPR ("personal data") ") in course of the activities according to Annex 1 (Section 1) of this Agreement. PROCESSOR shall refrain from any action contradicting its position as data processor and is bound by diligent compliance of the obligations of the applicable laws – especially but not exclusively according to the GDPR.

4.1.2. The PROCESSOR is obliged to demonstrable document the personal data processing according to the provisions of the GDPR. The PROCESSOR shall in particular keep records of processing activities as required according to Art 30 para 2 GDPR. The personal data processing shall be monitored by the person, which was entrusted with such monitoring at the PROCESSOR.

4.2. Instructions of the CONTROLLER

4.2.1. The PROCESSOR is obliged to process, transfer and use personal data and any processing results only according to CONTROLLER's documented instructions and for the purpose of performing the agreed services according to Annex 1 (Section 3) of this Agreement, unless required to do so by applicable law to which the PROCESSOR is subject. He is further obliged to return personal data to the CONTROLLER exclusively or transmit data exclusively after the CONTROLLER's prior written authorization. Such instructions are basically agreed in the Main Contract. Subsequent instructions can also be given by the CONTROLLER throughout the duration of the processing of personal data, but shall always be documented and kept in writing, including electronically, in connection with the main contract and this Agreement. The PROCESSOR hereby agrees that he may use the personal data processed solely on behalf of the CONTROLLER for his own purposes only with the consent of the CONTROLLER. PROCESSOR shall immediately inform the CONTROLLER if, in PROCESSOR's opinion, an instruction given by the CONTROLLER infringes applicable data protection provisions. PROCESSOR is entitled to refrain from further processing personal data until the CONTROLLER confirmed its instruction in writing. For the avoidance of doubt, PROCESSOR shall be entitled to analyze the processed personal data in order to optimize and improve its services.

4.2.2. The PROCESSOR shall process the personal data only to the extent required to perform the activities according to this Agreement and adhere to the principle of data minimization pursuant to Art 5 para 1 lit c GDPR. The PROCESSOR shall in particular ensure that the personal data of the data subjects according to Annex 1 and other PROCESSOR's own data or data of PROCESSOR´s clients is processed separately ("multi-tenancy").

4.3. Confidentiality

4.3.1. PROCESSOR shall grant access to persons only on a need to know basis. He confirms that all persons authorized to process personal data (direct or indirect access) or having potential access to data have been bound prior to accessing the data to confidentiality obligation pursuant to Art 28 Para 3 lit b GDPR and Sec 6 DSG. In particular, this confidentiality obligation shall persist even upon termination of their engagement and/or their professional relationship with the PROCESSOR. All persons who handle personal data are to be demonstrably trained in particular on the obligations according to GDPR and according to this Agreement. On request, the PROCESSOR shall demonstrate to the CONTROLLER that the concerned persons under the PROCESSOR's authority are subject to the abovementioned confidentiality.

4.4. Security of Processing

4.4.1. PROCESSOR declares that appropriate data security measures in particular according to Art 32 GDPR have been implemented to especially prevent data from being used contrary to regulations or that data will be made accessible to third parties. The currently implemented technical and organizational data security measures are listed in Annex 2 to this Agreement.

4.5. Data Subjects' Rights, Cooperation and Assistance

4.5.1. Taking into account the nature of the processing, PROCESSOR shall assist the CONTROLLER by appropriate technical and organizational measures, insofar as this is possible, with the fulfilment of the CONTROLLER's obligation to respond to requests for exercising the data subject's rights. PROCESSOR will provide CONTROLLER with the information required for this purpose.

PROCESSOR shall assist the CONTROLLER in ensuring compliance with the obligations pursuant to Art 32 to 36 GDPR while taking into account the nature of processing and the information available to PROCESSOR. The Processor confirms that technical and organizational measures enabling the CONTROLLER to comply with an obligation to notify the data subject and / or the supervisory authority according to Art 33 und 34 GDPR within statutory deadlines are in place. PROCESSOR shall especially notify the CONTROLLER without undue delay after becoming aware of a personal data breach and will provide the CONTROLLER with any information required for this purpose.

4.5.2. The PROCESSOR is obliged to comply with any request or request from the Data Protection Authority or other competent authorities and to adapt its internal data processing operations accordingly, regardless of whether such requests are made directly by the authority or through the CONTROLLER.

4.5.3. The Processor shall inform the Controller without delay of any request received from the Data Subject. He shall not respond to the request himself, unless he has been explicitly instructed to do so by the controller. The Processor shall assist the Controller in fulfilling the Controller's obligation to respond to requests from data subjects to exercise their rights. In doing so, the Processor shall follow the instructions of the Controller.

4.5.4. Any effort undertaken by the PROCESSOR for the CONTROLLER in order to assist the CONTROLLER in ensuring compliance with data subject's rights and further obligations of the CONTROLLER shall be subject to a remuneration based on the time and material used by the PROCESSOR. In general, an hourly fee of EUR 220,- (excl VAT) shall apply.

4.6. Erase and Return of Data

4.6.1. After the end of the provision of services relating to the data processing, PROCESSOR shall at the choice of the CONTROLLER either delete or return all personal data, documentation or any parts or copies thereof to the CONTROLLER and shall delete existing copies, unless applicable laws require a storage of the personal data by PROCESSOR. For the avoidance of doubt, PROCESSOR shall be entitled to retain statistical data concerning the processing.

4.7. Audit and Inspection

4.7.1. PROCESSOR shall make available to the CONTROLLER all information necessary to demonstrate compliance with the obligations laid down in Art 28 GDPR and allow for and contribute to audits, including inspections, conducted by the CONTROLLER or another auditor mandated by the CONTROLLER. When deciding on an audit, the CONTROLLER shall take into account relevant certifications of the PROCESSOR.

5. ENGAGEMENT OF SUB-PROCESSORS

5.1. CONTROLLER provides PROCESSOR a general written authorization in accordance with Art 28 (2) GDPR to engage other processors to conduct data processing activities ("**SUB-PROCESSORS**").

5.2. CONTROLLER specifically authorizes PROCESSOR to engage the SUB-PROCESSORS listed in Annex 3.

5.3. PROCESSOR shall inform the CONTROLLER of any intended changes concerning the addition or replacement of a SUB-PROCESSOR, thereby giving the CONTROLLER the opportunity to object to such changes pursuant to Art 28 Para 2 GDPR.

5.4. PROCESSOR shall enter into a written agreement with SUB-PROCESSORS and shall impose on each SUB-PROCESSOR all obligations of this Agreement. A copy of such Subcontractor agreements and subsequent amendments shall at the CONTROLLER's request be submitted to the CONTROLLER at least [4 weeks] in advance to enable CONTROLLER to ensure that the same data protection obligations as set out in this agreement are imposed on the Subcontractor. To the extent necessary to protect trade secrets or other confidential information, including personal data, PROCESSOR may blacken the relevant passages of the agreement before disclosing a copy. Further, the PROCESSOR ensures that the CONTROLLER may directly issue instructions directly to the Subcontractor, if this is necessary from a data protection perspective. If the Subcontractor does not fulfil his data protection obligations, the PROCESSOR shall remain fully liable to the CONTROLLER as regards the fulfilment of the obligations of the Subcontractor.

5.5. The Subcontractors outside of the EEA region can in any case just be engaged if (i) they are located in a third country that possesses an appropriate level of data protection rules that is accepted by a resolution of the EU-commission (decision of adequacy) or (ii) they have agreed upon EU-standard contractual clauses or equal contract templates that were issued by the EU-commission as appropriate guarantees pursuant to Art 46 para 2 lit c and d GDPR.

6. GOVERNING LAW AND JURISDICTION

6.1. This Agreement and its interpretation shall be governed by the law of the Republic of Austria with the exception of its conflict of laws rules and the UN Sales Convention.

6.2. For all disputes concerning the entering into, the realization, or the legal validity of this Agreement or concerning legal effects out of this Agreement the Parties agree that the competent Court of Vienna, Austria shall have exclusive jurisdiction.

7. FINAL PROVISIONS

7.1. This Agreement becomes effective as of the date of both parties' signature and is concluded for the validity period of the Main Contract. Considering the subject matter and nature of this Agreement the parties agree that every termination or expiry of the validity of the Main Contract also leads to a termination of this Agreement and is accompanied by similar consequences. This is not applicable to provisions whose content or nature implicate that they shall still be valid after the termination of the Agreement. The right to terminate this Agreement for good cause remains unaffected. A breach of this Agreement by the PROCESSOR or an objection to changes pursuant to Section 7.2. shall always constitute good cause for termination without notice. The PROCESSOR shall be entitled to terminate the

Agreement if the CONTROLLER insists on the fulfilment of its instructions after having been informed by the PROCESSOR that its instructions violate any applicable legal requirements pursuant to clause 4.2.1. In any case, any processing of personal data carried out on behalf of the PROCESSOR must be stopped immediately on the date on which the termination takes effect.

7.2. Amendments or supplements to this Agreement shall be made in writing, which may also be in electronic format. The Agreement including its Annexes shall be retained in writing, including electronically, by both parties.

7.3. Should any provision of this Agreement or a later amendment or supplement be or become invalid or unenforceable, then the validity or enforceability of the remainder of this Agreement shall not be affected. Any such invalid or unenforceable provision shall be deemed replaced by an appropriate provision, which, in accordance with the economic purpose and object of the provision and/or this Agreement, shall come closest to the Parties' original intention.

7.4. Any prior agreements, prior written or oral discussions, notices or undertakings or any oral subsidiary agreements cease to be in force upon signing of this Agreement. Amendments to this Agreement need to be in writing in order to be effective, unless there is a legally required stricter form.

Version: December 2023

[Date Stamp]

CONTROLLER	**PROCESSOR**
Name: [•]	Name: Gerhard Sigl
Function: [•]	Function: Chief Operations Officer

ANNEX 1

"FURTHER CONDITIONS OF THE PROCESSING"

1. PERSONAL DATA PROCESSED

1.1. PROCESSOR processes the following personal data on behalf of the CONTROLLER:

- User data of registered users:
  - First name
  - Last name
  - Email address
  - Password
- IP address of managed devices (Intercom stations, mobile apps, web-clients)
- Logfiles, especially configuration changes of claimed devices and systems, historical door calls with subsequent actions such as door open, role sharing, etc.
- Images, videos and audio processed via Symphony and stored in the cloud, transcripts of audio/voice recordings
- Video-Snapshots in case activated by CONTROLLER
- Pictures uploaded from CONTROLLER to be displayed at call buttons
- Contact List entries (Caller name as defined by the CONTROLLER)
- User Management on device
- Logs and Traces in case of Tech Support
- Any free form field entry if it contains personal data entered by the CONTROLLER

2. CATEGORIES OF DATA SUBJECTS

2.1. PROCESSOR processes personal data of the following data subjects on behalf of the CONTROLLER:

- Registered users (e.g. Owners, Administrators, Managed Users, etc.) on Symphony Cloud Platform (commend.services)
- Persons within the view area or acoustic range of the Symphony door call system
- Persons using the Symphony voice assistant functions

3. PROCESSING PURPOSE AS DETERMINED BY THE CONTROLLER:

- Configuration data of Intercom System
- Audio/Video data during Door Calls and Intercom Calls
- Audio data/recordings and transcripts during voice assistant calls
- User Reports (e.g. Audit trails, visitor report, etc.) as configured by CONTROLLER
- Tech Support
- Logging data to ensure availability of service as defined by SLA

ANNEX 2

"TECHNICAL AND ORGANIZATIONAL DATA SECURITY MEASURES"

Appropriate data security measures have been implemented to especially prevent data from being used contrary to regulations or that data will be made accessible to third parties. We are constantly improving our security measures in line with technological developments. The currently implemented technical and organizational data security measures are as follows:

ISO 27001 SECURE DEVELOPMENT COMPLIANCE

1. Secure Development Environment

- Azure Cloud
- Azure Security Center Monitoring
- Ansible Deployment based Infrastructure as Code (IaS)

2. Secure Source Control Management

- AD and Public-Key Authentication only
- Key Vault Secret Management
- Azure Artefacts Package Feeds
- Azure DevOps Git Repositories

3. Secure Software Management

- Compliance to Open-Source Software Policy
- OSS Vulnerability Management
- Component Change Management

4. Secure Software Design

- Compliance to Architecture Documentation Policy
- Compliance to SAFe Design Principles
- Compliance to Product Secret Policy

5. Secure Software Implementation

- Compliance to OWASP Top 10 Prevention Controls
- Compliance to OpenAPI Design Standard

6. Secure Software Coding Practices

- Compliance to Pull-Request based Code Review Policy
- Compliance to Code-Commit Policy
- Automated Static Code Analysis
- Automated Unit Testing Frameworks

7. Secure Software Integration and Testing

- Test Data Management through Staging Environment Dev-Prev-Prod
- Infrastructure as Code (IaS) Deployment
- DevOps CI/CD Pipelines
    - Build
    - Unit Tests
    - Vulnerability Monitoring
    - OSS Compliance Monitoring
- Automated Regression Testing
- Automated Heath Monitoring

8. Knowledge and Training

- Mandatory 4-eyes Code Review
- Deputy Concept

DEV-SEC-OPS BEST PRACTICES

1. High Availability

- Scripted Deployment for Infrastructure as a Service (IaaS)
- Slot-Swap Deployment for Platform as a Service (PaaS)
- Environment Segregation into Development-Preview-Production
- Automated Deployment Environment
- Automated Regression Testing
- Automated Health Monitoring
- Security Center Monitoring
- VoIP-System Redundancy

2. Integrity

- Azure AD DevOps Authentication
- Azure Key Vault Secret Management
- OAuth Identity and Access Management
- OAuth Cloud API Authentication
- Authentication using Certificates
- Public-Key-Infrastructure (PKI) for Device and Mobile Apps Certificates
- Device Specific Access Signature (SAS) Token for Firmware and Configuration

3. Confidentiality

- Encrypted Communication only
- Encrypted VoIP only
- Strong Secrets and Certificates
    - Framework with Secret Management Controls for Input, Validation, Storage and Authentication
    - Device and Mobile Apps Certificates

- Strong Cryptography
- Separation of Duties
    - Key Management vs. Usage

4. Security Best-Practices

- STRIDE-based Thread Modelling to Remediate Attack Vector
- Risked-based Assets Management incl. external/internal Interfaces

Defense-in-Depth Concept for Symphony and Concerto Platform

1. Physical Access Security

- Vandal resistant Station incl. Cameras
- Tamper contacts protect against vandalism
- USB-Port security by default

2. Network Access Security

- 802.1q VLAN Standard (Virtual Lan Segmentation)
- 802.1x Authentication Standard (RADIUS Server)
- IP-Secure Connector to cut the line to internal network

3. Data in Transit Security

- Encrypted communication and authenticated communication only
- TLS v1.2+ with Secure Cipher Suits only (>128bit)
- Device and Mobile Apps Identity Certificates
- X.509 v3 certificate secured communication and mutual device authentication

4. Data at Rest Security

- Azure Database and Storage via Platform as a Service (PaaS)
- Azure Storage Access with device specific SAS Token
- AES State-of-the-art data encryption (256 bit)
- SHA and BCRYPT salted password hashes (>256bits)

5. Open Source and Vulnerability Management

- Usage of de-facto Standard Libraries for Authentication and Encryption
- Contribution to Open-Source (e.g. Asterisk, BareSip, Mosquito, Wireshark)
- Continuous Vulnerability Monitoring

6. Device Endpoint Security

- Offline Availability incl. SIP call and door functions
- per device unique system credentials
- SSH remote Maintenance disabled by default
- SHA and BCRYPT salted passphrase and credential hashes (>256bits)

7. Device Application Security

- Offline Availability incl. SIP call and door functions
- Login Credentials change enforced on first login
- Login Credentials for 12+ character passwords
- Login Brute-Force Detection
- Network Port-Security

8. Mobile Application Security

- Offline Availability incl. SIP call and door functions
- Login Credentials for 12+ character passwords
- Secret Storage in Enclave
- Brute-Force Detection

9. Cloud Platform Security

- OAuth Identity and Access Management (IAM)
- Azure Key Vault Secrets Management
- Azure Storage Service Encryption (SSE)
- Azure Database Transparent Data Encryption (TDE)
- Azure Security Center Monitoring incl. ISO 27001 and Azure CIS Compliance

ISO 27001 certified ISMS

Additional Technical and Organizational Measures are defined and managed via Commend's Information and Security Management System (ISO 27001 certified!)

- Information Security Policy
- Risk Management Policy
- Classification of Data and Information
- Information Security Organization
- Asset Protection
- Network Security Policy
- User Access Management Policy
- Operational Security Policy
- Physical Security Policy
- Acceptable Use Policy
- Business Continuity
- Secure Development
- Security Incident Management

ANNEX 3

"SUB-PROCESSORS"

- Microsoft Corporation, Redmond, Washington, United States of America
- Auth0 Inc. Bellevue, Washington, United States of America
- Google Cloud EMEA Limited, Dublin 2, Ireland
- Elasticsearch B.V., Amsterdam, Netherlands

The list of SUB-PROCESSORS is also available on our website under https://www.commend.com/rd/cloud-privacy-policy-en