Agreement for the processing of personal data in the order in terms of art. 28 GDPR

between the

client or responsible

and

moveIT Software GmbH
(hereafter "**moveIT**")
(Contractor or processor)

1. SUBJECT AND TERM OF THE AGREEMENT

1.1 For the performance of the underlying contract (license contract) the contractor processes personal data ("**data**") on behalf of the client as a processor within the meaning of article 28 of the General Data Protection Regulation (EU) 2016/679 ("**GDPR**").

1.2 The term of this agreement starts by the client's signature of the underlying contract and ends after the termination or the quitting of the current contracts (e.g. maintenance contract for moveIT licences) and / or after the accomplishment of all contractually agreed work.

1.3 Subject of treatment: **moveIT licence products**

1.4 Type and purpose of treatment:

- **Installation and arrangement of moveIT licence products in the client's system via remote maintenance**
- **Other service works via remote maintenance in the moveIT licence products in the client's system (configuration, program and master data updates, troubleshooting)**

2. SCOPE OF ORDER PROCESSING

2.1 Categories of affected persons

The categories of persons affected by the treatment are:

- **Customers**
- **Suppliers**
- **Interested persons**
- **Employées**
- **Contact persons**

2.2 Type of processed data

The following types of data are subject of the processing of personal data:

- **Basic data about persons** (e.g. name, first name, gender, address)
- **Data about formation and profession** (e.g. acad. degree, job title)
- **Communication data** (e.g. phone, email)
- **Customer's history** (e.g. offers, orders, reclamations)

3. OBLIGATIONS OF THE CONTRACTOR

3.1 The data is processed exclusively in the context of a written order given by the client. The contractor processes the data exclusively in order to fulfill the services which are specified in the contract. The client allows the access to the data only to the extent which is necessary to carry out the contract.

3.2 If moveIT receives an official order to pass on the client's data and this order is legally permissible and refers to a given order, moveIT will inform the client immediately and will refer him to the inspecting authority.

3.3 The contractor must not correct or delete the processed data which was treated in the context of the data processing without the client's permission. Neither may he restrict the processing of the data. Only the documented instruction of the client can give him the authority to do so. If an affected person addresses the contractor directly in this regard, the contractor will forward this request immediately to the client, whereby further measures in the handling of the affected person are always the client's responsibility.

3.4 According to § 6 DSG 2018 (Austrian Data Protection Law, hereafter: "DSG") the contractor declares legally binding, that he obligates all persons commissioned with the data processing to confidentiality before starting the activity and that he will familiarize them with the data processing regulations which are relevant for them. In particular, this obligation of confidentiality remains valid for all persons commissioned with the data processing if they finish their duties or quit their positions in the contractor's company.

3.5 The contractor has to ensure the protection of the data through technical and organizational measures which satisfy the requirements of article 32 of the GDPR. moveIT complies with the technical and organizational requirements which are specified in the **appendix** of this agreement. It has to be pointed out that the client and the contractor perform additionally to the content of this agreement for the processing of personal data in the order the legal duties related to articles 28 to 36 of the GDPR.

3.6 The contractor reviews regularly the internal processes and the technical and organizational measures in order to ensure that the processing within his area of responsibility complies with the requirements of the applicable regulation of data protection and that the protection of the rights of the affected persons is guaranteed.

3.7 The contractor can extend and improve the measures in accordance with the contract. This can lead to a replacement of certain measures by other measures which are at least as effective as the other ones and aim the same goal. In order to make significant changes, the contractor needs a written agreement with the client.

3.8 If the contractor receives a request for information and the contractor is erroneously considered as the client of the data application in use, the contractor will immediately forward the request to the client and will inform the requester about it. The contractor undertakes to support the client as far as possible by using appropriate technical and organizational measures, so that the client may respond to the requests of affected persons according to the persons' rights in terms of chapter III of the GDPR, if this request refers to an order for processing data given to the contractor by the client.

3.9 On request, the client and the contractor cooperate with the supervisory authority in the fulfilment of their duties.

4. AUTHORITY AND RIGHTS OF THE CLIENT

4.1 The contractor will process the data exclusively according to the documented instructions of the client. In case of an oral instruction, the client will immediately confirm the instruction in writing. If the contractor considers that an instruction violates the GDPR, the DSG 2018 or other data protection regulations, he will inform the client without delay. The contractor is not obliged to follow obviously illegal instructions.

4.2 The client has the right to assure himself at any time on the basis of all necessary information of the contractor's compliance with data protection regulation. The client will minimize the impact of the control on the contractor's business.

5. DELETION OF DATA

5.1 The termination of the contractually agreed work has to be recorded by a written confirmation of the client. After the termination of the order or earlier upon request by the client, the contractor returns the data stored for processing to the client or he deletes the data completely and professionally in response to the client's request, unless otherwise agreed. The deletion has to be confirmed to the client in writing.

5.2 The obligation of deletion does not apply if the contractor has a legal obligation to store the corresponding personal data. In this case, the contractor may retain the data according to the respective retention periods (especially according to commercial or tax law) beyond the end of the contract and may destroy them in accordance with data protection only after the expiry of the respective retention periods.

6. SUB-ORDER RELATIONS

6.1 If the contractor charges another processor in order to process an order given by the client (in a specific case), this requires the written consent of the responsible. Consequently, the other processor is contractually subject to the same data protection obligations established between moveIT and the responsible person in the framework of the agreement for the processing of personal data in accordance with art. 28 of the GDPR.

6.2 For the purposes of this regulation, subcontracting does not include services such as telecommunication services, postal/transport services, maintenance and user services or the disposal of data media and other measures which shall ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment.

7. FINAL PROVISIONS

7.1 The contractor may claim a fee for support services which are not included in the service description of the order placed by the client or which are not attributable to a mistake of the contractor.

7.2 moveIT has no data protection officer within the company. According to article 37 GDPR, this is not mandatory for moveIT.

7.3 The foundation for the application of the GDPR is based on Austrian law (DSG 2018). Place of jurisdiction is Wels.

7.4 This agreement supplements the contract to which it relates.

7.5 If it should be or become necessary to make changes to this agreement in order to fulfill the requirement of the GDPR or the supplementary or concretizing national data protection regulations, the parties undertake to adapt it. A change, supplement, abolition or a termination of this agreement as well as the amendment of this clause must be in writing.

For the client:

____
Company

____
Place | Date

____
Signature

____
Name in fair copy

For the contractor:

moveIT Software GmbH
Company

Wels, 18. April 2018
Place | Date

ppa.
Signature

Kevin Hornung, MSc, Verantwortlicher für Datenschutz
Name in fair copy

ATTACHMENT TO THE ANNEXE

Technical and organisational measures in terms of article 32 (1) GDPR

1. Guarantee of confidentiality

a) Access control to the building

Technical or organizational measures to prevent unauthorized access to the premises where the data is processed:

- Visitors are picked up by the visited person directly at the entrance area of the building. Furthermore, the visited person leads the visitors to the appropriate place in the building. At the end of the visit, the visited person leads the visitors to the exit.
- The main entrance which leads to the premises of moveIT is closed. You need a key to open it. Only IT staff with a key has access to the server rooms. The server rooms are always closed.
- Alarm protection of windows and entrance doors.

b) Access control to the systems

Technical or organizational measures to prevent unauthorized use of the data processing systems:

- The access to the data processing systems is only possible by means of a user ID and a personal password assigned within the domain
- The user ID is automatically blocked after five incorrect password entries. Only the system administrator can lift the lock by a defined authentication process. All user ID locks are logged and regularly monitored by the system administrator.
- The servers are protected by a firewall in order to prevent external access.

c) Access control

Technical or organizational measures to ensure that persons who are authorized for the use of a data processing system only have access to the data within their access authorization and that personal data is not read, copied, altered or removed during processing, use or after storage:

- The personal employee ID with the individual employee password is used to access special programs that grant access to the necessary program sequences according to their personal authorization.
- The system administrator assigns personal employee IDs in order to control the access authorization.
- The system administrator can, on instructions, control the accessibility through password deletions or modifications and allocation of priorities.
- The access to the server systems is restricted to employees with the appropriate administrator rights.
- In the context of remote maintenance, a security token is used in order to connect to the client's system. If the client has no such security token, a remote maintenance tool is used for the connection.

d) Transfer control

Technical or organizational measures to ensure that personal data cannot be illegally read, copied, altered or removed during the electronic transmission, the transport or the storage on data carriers. Furthermore, these measures make it possible to check and determine to which places a transfer of personal data will take place or has taken place by means of data transmission:

- In the framework of the data protection regulations, a qualified specialist company destroys the data carriers which are no longer required physically (including those in paper form) and it disposes the data carriers in accordance with the data protection laws.
- In general, only employees of IT with appropriate authorization have access to data carriers.
- Tapes with backup files are created by the system daily.
- Backup data media are stored externally and they are deleted regularly.

2. Guarantee of integrity

a) Input and back up control

Technical and organizational measures to ensure that it is possible to verify and determine subsequently if and by whom personal data has been entered, altered or removed from the data processing systems:

- Only authorized persons may delete stored data.

b) Separation control or appropriation control

Technical and organizational measures to ensure that data which was collected for different purposes can be processed separately:

- The database systems of moveIT separate logically the data which was collected for different clients and different purposes. As a result, the data can only be read, edited and changed by the employees with the appropriate rights.

3. Availability and resilience

a) Availability control

Among other things, the contractor will take the following technical and organizational measures to ensure that personal data is protected from accidental destruction or loss:

- The building and the IT centre are protected against damages which are resulting from a lightning strike.
- The fire alarm is reported via a central fire alarm system which is connected to the fire brigade and the police 24 hours a day and 365 days a week.
- In the framework of data backup, the back-ups of the databases are regularly created and outsourced by the productive systems. During operation, the data is stored on Raid systems or mirrored database systems.
- Fire alarm system, UPS in the IT centre

b) Rapid recoverability (Art. 32 para. 1 lit. c GDPR);

- Backup of the CRM systems once a day on a virtual machine, easy and fast recoverability due to tape backup
- Backup of the internal client-related file storage with group policy access protection once a day (triple backup): on two different virtual servers and on tape, fast recoverability due to snapshot backups
- The client is responsible and liable for a central data storage provided by the client himself (e.g. Transfer Cloud)

c) Resilience

Measures to ensure the resilience of systems and services related to the processing.

- All data which is entered into the client’s system is already stored in the background database during the process of entering (on demand).

4. Pseudonymization and encryption

- The access to our database systems (CRM, projects, errors, etc.) outside the company is only allowed via a protected VPN connection. In addition, the user must be enabled by our IT for VPN access before a connection is possible. Our internal database systems are additionally signed by Lotus Notes certificate.
- Company notebooks are protected by Bitlocker (encryption of the hard disk) and are not readable in case of loss or theft.
- Company mobile phones and tablets can be blocked and deleted remotely in the event of loss or theft.
- Emails sent within moveIT are encrypted by default.

5. Procedures of regular reviews and evaluation of the effectiveness of the technical and organizational measures

- Incident-Reponse-Management
- Trainings for employees
- The databases in the background of moveIT@ISS+ are always state-of-the-art, guaranteed by ongoing maintenance contracts with the software supplier Progress (current version Progress 11.7). All the frameworks (Windows components) which are used for moveIT@ISS+ are also state-of-the-art, as well guaranteed by ongoing maintenance contracts (Visual C++2015 and .Net 4.X). Due to the internal quality assurance at moveIT, setup tests are carried out at regular intervals.
- There will be no order data processing in terms of art. 28 GDPR without corresponding instructions of the client, e.g. clear contract design.