EASY SOFTWARE

Contract on Processing Personal Data on Behalf of a Controller

made and entered into by and between EASY SOFTWARE Deutschland GmbH, Am Hauptbahnhof 4, 45468 Mülheim an der Ruhr hereinafter referred to as "Processor (Contractor)" and the customer hereinafter referred to as "Controller (Principal)" as named in the order confirmation or in the offer.

Preamble

This "Contract on Processing Personal Data on behalf of a controller " (hereinafter referred to as Agreement) substantiates, above all, the obligations of the contracting parties referring to privacy in conjunction with the Processor's handling of the Principal's or his customer's personal data (hereinafter referred to as Data). The privacy provisions of this Agreement **(**§ 1 to § 8) apply to all activities in which employees of the Processor or the Processor's agents are processing data on behalf of the Controller, or encounter data. Additionally, the Processor shall be provided, as part of the main contract or other business relations between the parties, confidential information from the Controller's organization, or it is not precluded that the Processor encounters such information in the Controller's business rooms.

§ 1 SUBJECT, TYPE, SCOPE, PURPOSE, AND DURATION OF ORDER PROCESSING

1.1. Type, scope and purpose of data processing will be substantiated in **Exhibit 1**. The Processor may only process the categories of data named in Exhibit 1 of the people affected that are named there for the purposes named there or in a possibly exis ing main contract. The existence of a possible main contract is set in Exhibit 1.

1.2. Other substantiations with regard to purpose and people affected regarding differing orders will be regulated in additional exhibits to this contract.

1.3. The Processor is not allowed to survey or use any data diverging or exceeding the above data, particularly the use of data for his own purposes.

1.4. The duration of this Agreement applies to the duration of an existing contractual relationship, particularly an existing maintenance contract, or a possibly existing main contract.

§ 2 CONTROLLER'S RESPONSIBILITY AND RIGHTS OF INSTRUCTION

2.1. As part of this Agreement, the Controller shall be responsible for complying with the legal privacy provisions in respect of people affected and third parties. The Controller's responsibilities pursuant to Clause 28 paras. 10, 82, 83 and 84 of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter referred to as **GDPR**) shall remain unaffected. In the mutual relationship of he parties, the Controller is the owner of the data and the owner of all rights to that data.

2.2. The Processor shall only process data on behalf of the Controller and to the documented instructions of the Controller, pursuant to Clause 28, 29 GDPR unless the Processor is required to process data by applicable law; in such a case, the Processor shall inform the Controller of this prior to processing it unless applicable law prohibits such notification due to important public interest.

2.3. The instructions will be initially defined by Exhibit 1 and this Agreement; the Controller may then substantiate, modify, supplement, or replace them in text form through individual instructions (individual instruction). In urgent cases, instructions may also be made orally; confirmation of this instruction in text form will in such cases be subsequently made. In this regard, the Controller has an extensive right of instructions about type, scope, and purpose of processing data.

2.4. The Processor must confirm and document individual instructions at least in text form.

2.5. If the Processor is of the opinion that an instruction violates applicable privacy laws, he will immediately inform the Controller of this.

§ 3 PROCESSOR'S DUTIES

3.1. The Processor may process data only as part of the Controller's order and instructions, and only within the territory of the European Union (EU) and European Economic Area (EEA). The Processor shall use the data for no other purposes than fulfilling the main contract. The Processor may not hand over data without the Controller's prior written consent to hird parties of other recipients. Data transfers to subcontractors pursuant to § 6 para. (2) second HQ remain unaffected by this.

3.2. The Processor shall build his internal organization in his area of responsibility in such a manner that it meets the special data protection requirements. The Processor shall undertake technical and organizational measures (TOM) pursuant to Clause 28 para. 3 lit. c, Clause 32 in combination with Clause 5 paras. 1 and 2 GDPR to protect the Controller's data and maintain these for the duration of this Contract not later than by the beginning of processing data. The current state of technology must be observed here, taking the risk into account. These measures will be defined in **Exhibit 3**. The Processor will be allowed to modify the measures taken if it can be guaranteed that this does not fall short of the agreed protection level. In case of essential modifications, he Controller shall be informed in writing of the modification intentions of the Processor prior to implementing them. The Processor shall furnish evidence of complying with these measures by submitting documentation material on demand.

3.3. The Processor ensures and routinely checks that processing data in his area of responsibility, which includes possible subcontractors, be made in accordance with the provisions of this Agreement and the Controller's instructions and that the technical-organiza ional measures be complied with. The Processor shall be obliged to document these checks and submit them to the Controller upon the latter's demand.

3.4. Unless his is already the case, the Processor must oblige all people involved with processing the data to secrecy pursuant to GDPR in writing unless these people are already subject to comparable, even legal, professional secrecy. The Processor must instruct these people to the essential legal provisions on data protection, and oblige them to comply with these provisions. The Processor shall, upon the demand of the Controller, provide evidence by submitting the formal obligations.

3.5. The Processor ensures to appoint a data protection officer and, at least for he duration of this Agreement, employ that officer. The name of the data protec ion officer and the contact data can be obtained from the Processor's home page (www.easy de).

3.6. The Processor shall support the Controller, taking the type of processing and the information available to him into account, when complying with he Controller's duties arising from Clause 32 GDPR (TOM), from Clauses 33 and 34 GDPR (obligations to report in case of data breaches) and, where necessary, from Clause 35 GDPR (data protection impact analysis), as well as Clause 36 GDPR (consulting the regulatory authority).

3.7. The Processor shall provide the Controller all required information for proving compliance with the duties defined in Clause 28 GDPR.

§ 4 QUERIES BY PEOPLE AFFECTED

4.1. In case people affected assert justified privacy claims from the Controller, the Processor will support the Controller, taking the type of processing into account, with appropriate technical and organiza ional measures, where possible, in meeting these claims.

4.2. In case people affected immediately consult the Processor to assert their rights, the Processor will immediately forward this request to the Controller. The Processor will, in particular, not answer any requests by people affected for information.

§ 5 SUPERVISION RIGHTS OF THE CONTROLLER

5.1. The Controller is authorized, prior to starting to process data and then rou inely, to check the technical and organizational measures taken by the Processor. The Controller shall document the result of these checks. For this purpose, the Controller may obtain, for example, informa ion by the Processor or check on-site in the premises of the Processor during normal business hours, or have a third party to carry out these checks.

5.2. The Processor shall grant the Controller or a third party commissioned by the latter access, information and inspection rights required for performing the checks, and shall actively make an appropriate contribution to performing those checks.

§ 6 SUBCONTRACTORS

6.1. The Processor may entrust suitable subcontractors from the EU or EEA territory with processing data on behalf of and to instruction of the Controller if the Controller has given his consent to this in writing and prior to commissioning the subcontractor. The Processor will inform the Controller of any intended change with regard to involving or replacing subcontractors. The Controller may contradict the involvement or replacement of subcontractors upon information given by the Processor. A contradiction may only be made for good cause.

6.2. The subcontractor must be subjected to the same privacy obliga ions defined in this contract. In particular, the Processor must ensure that the appropriate technical and organizational measures are performed by the subcontractor in such a manner that processing is performed according to the requirements of data protection legislation. In the subcontractor contract, the Controller must be immediately granted all supervision rights with regard to the subcontractor pursuant to § 5 within the meaning of a genuine contract on behalf of third parties.

6.3. The Controller may prompt the Processor to provide information about the subcontractor's privacy related obligations and to grant inspection of the relevant contract documents.

6.4. If the subcontractor does not meet his privacy obligations, the Processor will be liable to the Controller with regard to meeting the subcontractor's obligations.

6.5. The subcontractors listed in **Exhibit 2** are approved.

6.6. Services that the Processor claims with third parties as an additional service in support of carrying out the order are not subcontractor relations within the meaning of this provision. These include, for instance, telecommunications services, maintenance and user service, cleaning staff, auditors, or disposal of data media. However, the Processor is obliged to make appropriate and legally compliant contractual agreements and to take supervision measures to ensure protection and security of the Controller's data, even in case of additional services assigned to third parties.

§ 7 SPECIAL OBLIGATIONS FOR THE PROCESSOR IN CASE OF "DATA BREACHES"

7.1. The Processor shall immediately notify the Controller in case of violations of privacy regulations or this Agreement on the part of the Processor or of the people employed with him as part of the contract if there are clues that data has been improperly processed. This does not affect § 3 para. (7). Additionally, the Processor shall take the required measures to secure the data and to diminish possible consequences to the detriment of those who are affected.

7.2. If the Controller's data become endangered with the Processor through forfeiture or requisition, an insolvency procedure or other events or measures by third parties, the Processor must immediately inform the Controller of this. The Processor shall immediately inform all those responsible in this connection that sovereignty and ownership of the data is exclusively with the Controller.

§ 8 RETURNING OR DELETING DATA MEDIA OR DATA

8.1. The Processor immediately corrects, deletes or blocks the data when so instructed by the Controller. The Processor shall be in charge of deleting privacy compliant data or destroying data media based on a single order by the Controller unless this has already been agreed in a possible main contract. Single orders for deletion is not required in case of test or scrap materials. Legal retention obligations remain unaffected.

8.2. The Processor has to delete and/or return data selected by the Controller after the end of the contract unless the Processor is obliged to save data due to other provisions. The Processor does not have any rights of retention for the data unless his counterclaim has been found to be valid or undisputed.

§ 9 Written form, relationship to main contract, choice of law

9.1. Changes and amendments to this Agreement require a written agreement. This also applies to statements waiving the obligation to use this form.

9.2. In case of possible objections, provisions of this Agreement will override the provisions of a possibly existing main contract.

9.3. The laws of the Federal Republic of Germany apply.

EXHIBIT 1

PURPOSE, TYPE, AND SCOPE OF DATA PROCESSING, TYPE OF DATA AND GROUP OF PEOPLE AFFECTED

PURPOSE OF PROCESSING

- Install software at Controller's site
- Maintain and supporting the installation at Controller's site
- Remotely maintain he installation at Controller's site

TYPE AND SCOPE OF PROCESSING

- Access data as part of remote access
- Cache while remotely access data
- Display data as part of remote access
- Create a support ticket for failures at Controller's site
- Keep a project file with regard to Controller's installation
- Controller accessing the extranet for information

TYPE OF DATA

- First and last names
- Dates of birth
- Addresses
- E-mail addresses
- Telephone numbers
- IP addresses
- Personnel files

GROUP OF PEOPLE AFFECTED

- Controller's customers
- Controller's employees
- Controller's potential customers and prospects
- Controller's vendors

EXHIBIT 2

SUBCONTRACTORS APPROVED IN ADVANCE

- EASY SOFTWARE AG, Am Hauptbahnhof 4, 45468 Mülheim an der Ruhr, Germany
- OTRIS Software AG in Dortmund, Königswall 21, 44137 Dortmund, Germany
- CTO Balzuweit GmbH, Lautlinger Weg 3, 70567 Stuttgart, Germany
- I.R.I.S. AG, Heusstraße 23, 52078 Aachen, Germany
- Contellix GmbH, Mainzer Landstraße 41, 60329 Frankfurt, Germany
- friendWorks GmbH, Theresienplatz 31, 94315 Straubing, Germany
- SAP Deutschland SE & Co.KG, Rosenthaler Straße 30, 10178 Berlin, Germany

EASY SOFTWARE

EXHIBIT 3

TECHNICAL AND ORGANIZATIONAL MEASURES

CONFIDENTIALITY
(i.e. data is not accessible to unauthorized persons)

POLICIES:
- Privacy policies determine how to handle personal data in concrete cases.
- Secure handling of software and hardware as well as security measures to be adhered are defined as part of IT security policies.

TRAINING:
- Employees routinely receive training courses on data protection and for information security.

PHYSICAL ACCESS CONTROL ("ZUGANGSKONTROLLE"):
(prevents granting unauthorized persons physical access to the processing facilities/rooms for personal data or other people-related documents, e.g. files or data media)

- Access control to buildings or external offices is granted either via cards or via keys.
- Cards contain a picture without naming he company name
- Access to internal data centers has additional security. Only employees with the corresponding rights may enter this area.
- The company's data center is located at the Mülheim headquarters. This building is secured with an alert system that is directly connected to a security service. Until the end of year 2018 we will outsource our hardware equipment to an external data center with ISO 27001 certification. A data processing agreement was signed.
- In case of external data centers, we take care to ensure cer ification to ISO 27001 and effective measures for access control.
- Visitors to the HQ must register and will receive a visitor's card. In external offices, they will have to contact an employee, so a check is made According to IT security policy, visitors may not linger unaccompanied in the building.
- Sensitive data media and paper files are kept in lockable filing cabinets.

ACCESS CONTROL / USER CONTROL:
(prevents that unauthorized persons can use the DP systems in which personal data is processed, e.g. user/password provision)

- Access to DP applications requires personalized login with dedicated user rights.
- Passwords must have a length of 12 characters and should contain uppercase and lowercase letters as well as numbers.
- Passwords are saved hashed.
- The number of login attempts to the domain is limited.
- User accounts that are no longer used are immediately disabled.
- Access to company resources wi hout authentication is not possible.

ACCESS CONTROL / STORAGE CONTROL / DATA MEDIA CONTROL:
(guarantees that authorized users can only access the data and functions underlying their access permission, e.g. through role/permission concepts)

- A Microsoft Active Directory is used as the basis for granting rights. Here, the rights are granted to individual network resources using group assignments. Where possible, other software products are connected to the AD. Usually all products used provide the capability of differentiating rights by crea ion, reading, writing, and deleting.
- Rights to resources are granted only as and when required.
- Rights must be requested via the internal IT support's ticket system. These are only granted after the corresponding supervisor has confirmed.
- All data media are encrypted according to IT security policy. By deleting he corresponding keys, the data is also securely deleted from SSD data media. When selling or retiring, data media will be deleted once again.
- Paper shredders are available for destroying paper documents. For larger quantities, a container of a correspondingly certified service provider will be requested for destruction.

SEPARATION RULE / SEPARABILITY:
(guarantees that personal data collected for different purposes can be processed separately, e.g. by system or client separation, etc.)

- Data from different Controllers is logically separated by granting permissions; it can also be deleted and viewed separately.
- Only client-enabled systems or systems with logical separability will be used.

ORDER CONTROL ("AUFTRAGSKONTROLLE"):
(guarantees that personal data processed on order can only be processed according to the Controller's instructions)

- Surveying, processing, correcting and deleting data is performed strictly bound to the order and individual instructions by the Controller according to the contractual agreements made here.
- subcontractors are carefully selected, taking Clause 11 of the German Federal Data Protection Act or Clause 28 of GDPR into account and thus suitability of the technical and organizational measures taken by them.
- Orders and, in conjunctions with them, ordering (data) processing agreements are in writing.
- Contracts with subcontractors in third countries are precluded by the application of EU standard contractual terms.
- Employees and subcontractors used where access to personal data cannot be precluded shall be bound to data secrecy or confidentiality in writing.

ENCRYPTION:
(guarantees that particularly sensitive, personal data can only be accessed through knowledge of a specific decryption code.)

- Notebooks, smartphones, USB sticks and other mobile data media containing the Controller's data are encrypted. For this purpose, we use Bitlocker on Windows or Filevault on MacOsX.
- For creating encrypted containers, we use the OpenSource application Veracrypt. Any employee can install this when needed.
- When using Web applications, we ensure for exclusive accessibility via HTPPS.
- We provide employees with a VPN to enable them to use a secure network connection when on external business.

ANONYMOUS / PSEUDONYMS:
(guarantees that iden ifying a specific person is avoided or made more difficult if identifying that person is not absolutely necessary for the purpose of processing the personal data – "data avoidance".)

- Wherever useful and possible (e.g. for statistics), personal data will be given pseudonyms or be anonymous.

INTEGRITY
(i.e. data cannot be adulterated)

EASY SOFTWARE

TRANSPORT CONTROL / TRANSMISSION CONTROL (DISSEMINATION CONTROL):

(guarantees that personal data cannot be read, copied, modified or removed by unauthorized persons when disseminating it, i.e. transmitting or transporting it, e.g. by transport encryption)

- Access to Web-based DP systems in which personal data is processed is only possible via encrypted communication connections (https and TLS).
- Remote access to the internal IT network from IT systems outside of the internal net is only via VPN technology.
- Inbound and outbound data traffic is monitored using a firewall appliance. Time, content, recipient and the ini iating sender of data transmissions are logged.
- Secure transport containers/packages are used for physically transporting personal data. Transport personnel and vehicles (e.g. for courier services) are carefully selected.
- Data media used for transport must be encrypted.

INPUT CONTROL ("EINGABEKONTROLLE"):

(guarantees that subsequent checks and determinations can be made on which personal data has been entered into automated processing systems or modified at what time and by whom, e.g. by logging)

- Inputs into and modifications to relevant application systems are recorded and monitored via logs/log-files where traceability of input, modification and deletion of data (content and time of modification) as well as the executing user (through individual user names, not user groups) are guaranteed.

AVAILABILITY, CAPACITY / RESILIENCE, RECOVERABILITY

(i.e. data is available when needed)

AVAILABILITY CONTROL ("VERFÜGBARKEITSKONTROLLE"):

(guarantees that personal data is protected from destruction or loss, e.g. through fire precautions, etc.)

- The servers are secured against power outage via a USV.
- We use virtualization solutions for servers, so in case of failure of individual engines the system can continue running on another instance.
- The server rooms are air-conditioned.
- Modern fire precautions and alert systems are used. Automatic gas extinguishers prevent on-going damage.

CAPACITY (IN THE SENSE OF RESILIENCE):

(guarantees that the IT systems are resilient to attacks)

- All DP systems on which the agreed services are running are protected by a firewall from external access.
- Updates must be loaded quickly into all systems when available. Automa ic update mechanisms are preferred.
- All systems are equipped with anti-virus software.
- Use of intrusion detection systems in the central firewall.
- Response time behavior of essential systems is routinely monitored to enable early identification of extraordinary load situations (e.g. through cyber-attacks) and thus possible failure of the systems.

RECOVERABILITY:

(guarantees that systems used can be recovered in case of failure)

- The backups routinely created automatically in different generations are kept redundant in different parts of the building.

ENSURING PERMANENT EFFECTIVENESS OF THE MEASURES TAKEN:

(guarantees that measures taken are routinely checked and, when needed, customized)

- Proper retention and performance of the measures listed here is manually and/or DP logged (burden of proof)
- All measures listed here are subject to routine reviews; they are continually improved.