



# EASY SOFTWARE

## ORDER DATA PROCESSING AGREEMENT WITH EASY SOFTWARE AG

### § 1 SUBJECT OF THIS AGREEMENT

- 1.1. Subject of this Agreement is the processing of personal data by EASY SOFTWARE AG (hereinafter referred to as EASY) on behalf of the Customer (cf. Section 11 German Data Protection Act - BDSG) and for the purposes of the contract concluded between both parties regarding the installation and configuration of the provided software, customization of standard software as well as software maintenance, support by EASY and provision of professional services by EASY for the customer. The Customer remains the sole owner and master of any data processed by EASY. All rights and obligations pursuant to BDSG are incumbent upon the Customer. EASY shall process personal data on behalf of and only according to the instructions from the Customer.
- 1.2. The Customer has contracted EASY, in particular, to provide services regarding the maintenance of software.

Order data processing affects the following:  
employees, vendors, and the customer's clients or other affected parties.

Categories of personal data for order data processing are:  
first name, last name; if necessary, department, contact data, invoice information, e-mails or other data.

### § 2 PROCESSING, COMPLIANCE WITH DATA PROTECTION

- 2.1. EASY shall process personal data and other information on behalf of the Customer pursuant to Section 11 BDSG.
- 2.2. EASY shall undertake to comply with all applicable data protection provisions, in particular the BDSG and the data protection provisions laid down in the German Telemedia Act (TMG) and the German Social Security Code Volume 1 (SGB I).

### § 3 DATA SECRECY, COMPLIANCE WITH INSTRUCTIONS

- 3.1. EASY warrants complying with the data secrecy obligations pursuant to Section 5 BDSG when processing the personal information and other information.
- 3.2. EASY shall process personal information only within the context of and according to the instructions by the Customer.
- 3.3. Correction, deletion and blocking of personal information shall only take place upon instruction by the Customer as long as the parties have not agreed otherwise in writing.

### § 4 EASY'S STAFF

- 4.1. EASY shall choose the staff entrusted with the processing of personal information diligently and shall review their reliability periodically.
- 4.2. Additionally, EASY shall bind such staff to confidentiality pursuant to Section 5 BDSG before entrusting them with personal data protection related tasks.

### § 5 SUBCONTRACTORS

- 5.1. EASY shall use subcontractors only upon prior written notice by the Customer and shall bind them to the principles of data protection according to this agreement. Currently, EASY employs the subcontractors named in Appendix 1 to this Agreement for processing data; the Customer already consents to the use of these subcontractors by entering into this Agreement.
- 5.2. EASY shall choose subcontractors diligently and under consideration of their reliability in the context of handling personal information. Furthermore, EASY shall periodically review the subcontractor's reliability as required by data protection regulations.

### § 6 SECURITY CONCEPT, SUPERVISION RIGHTS

- 6.1. The Customer is solely and exclusively entitled to direct the use and handling of the personal information processed by EASY and may review the EASY's compliance with his instructions.
- 6.2. EASY shall implement the required technical and organizational measures for the protection of personal information, in particular against unauthorized access as well as loss of and damage to the data. The security measures to be implemented by EASY are set out in Exhibit 2.
- 6.3. The Customer is entitled to reasonably review EASY's compliance with the data protection obligations laid down in this Agreement. EASY shall reasonably assist the Customer with such review, in particular by granting access to rooms, systems and documents. For this purpose, the Customer is also entitled to consult EASY's employees. Hereby incurred costs of EASY shall be borne by the Customer to a reasonable extent.
- 6.4. The Customer may inspect EASY's files and control devices related to the performance of this Agreement. In case of any violation of data protection, the Customer may request EASY to implement reasonable measures.
- 6.5. As the Customer requests reviewing EASY's documents, data, systems or other areas which contain business secrets or other client's data, EASY may demand that such review is carried out by an independent third party.
- 6.6. The Customer shall notify EASY of its wish to conduct an inspection or review within a reasonable notice period of at least four (4) weeks. The Customer shall ensure that reviews and/or inspections do not unreasonably affect EASY's ongoing business operations. The Customer has to bear the costs for supporting services, provided by EASY in case of reviews and/or inspections.

### § 7 STATUS INFORMATION/OVERVIEWS

At the Customer's request, EASY shall produce an overview of all data processing conducted by EASY and hand over such overview to the Customer. This may involve the following fields:

- Data processing systems being used;
- Categories of data processed;
- Recipient of any transferred data, if transfer is contractually agreed;
- Individuals or groups of persons that have the right to access the data.



# EASY SOFTWARE

## § 8 DATA PROTECTION OFFICER

- 8.1. EASY has appointed a data protection officer. Pursuant to the applicable statutory regulations, the data protection officer is obliged to work towards the compliance of data protection regulations, in particular to monitor the proper application of data processing software and to train employees who have access to personal information.
- 8.2. The data protection officer is directly subordinated to EASY's management and not bound to instructions that may inhibit exercising his duties as data protection officer. EASY shall name the data protection officer on Customer's request; EASY will inform the Customer about any changes within reasonable time.

## § 9 REPORTING REQUIREMENTS, DATA PROTECTION DISRUPTIONS AND VIOLATIONS

- 9.1. EASY shall immediately notify the Customer of disruptions in processing and/or suspected data protection violations or other irregularities in the context of data processing. This applies in particular to any unauthorized or unintended access to the personal data processed by EASY on behalf of the Customer and/or in cases of unauthorized transfer.
- 9.2. Reporting requirements already apply if there is the danger of prospective disruptions, violations or irregularities.
- 9.3. The Customer shall also notify EASY of any disruptions or other irregularities it becomes aware of.

## § 10 TERMINATION

Upon termination of this Agreement, EASY shall immediately return all personal information processed on behalf of the Customer in a common digital format to the Customer. This also includes the data created for the purposes of backup and logging. The Customer shall confirm the return of the data. Subsequently, EASY shall delete the Customer's data immediately, except where EASY is obliged to archive the data according to statutory regulations; in this case, EASY shall block the data and use it only for the legal purposes according to this Agreement.

## § 11 FINAL PROVISIONS

- 11.1. Should any provision of this agreement be or become invalid or illegal, the remaining provisions shall remain binding.
- 11.2. The jurisdiction for any disputes arising from this Agreement depends on the jurisdiction laid down in the main contract.

## APPENDIX 1 – Subcontractors

Subcontractors with whom contracts for order data processing have already been concluded for a subcontract:

- EASY SOFTWARE Deutschland GmbH, 60323 Frankfurt/Main
- EASY Enterprise Services GmbH, 45468 Mülheim/Ruhr
- 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
- friendWorks GmbH, Theresienplatz 31, 94315 Straubing, Germany
- Lubrich IT Consulting, Talhauser Straße 60a, 79285 Ebringen, Germany
- Contellix GmbH, Mainzer Landstraße 41, 60329 Frankfurt, Germany
- WMD Vertriebs GmbH, Ahrensburg, Germany



# EASY SOFTWARE

## APPENDIX 2 - SECURITY CONCEPT

### Technical and organizational measures according to the Annex to Section 9 BDSG

#### 1. Physical Access Control ("Zutrittskontrolle")

The access to the building is only possible via an entrance that is constantly staffed by an employee. In addition, every employee has a chip card which grants access to the rest of the building. The computer systems are located in a closed area, which is only accessible by staff of the IT department. Out of business hours, the building is secured by an alarm system which is directly connected to a security service.

#### 2. Electronic Access Control ("Zugangskontrolle")

Every employee has its own user identification with password which controls the access to the computer systems. The connection to the internet is secured by a firewall. External access by employees to the company network is secured by a VPN.

#### 3. User Access Control ("Zugriffskontrolle")

Microsoft Active Directory is used in order to grant different levels of access to the resources. Employee access is restricted to those resources which are necessary for his/her operation. In addition, all client computers contain data carrier encryption which prevents unauthorized access to stored data.

#### 4. Disclosure Control („Weitergabe-Kontrolle“)

It is determined by process instructions that data carriers need to be encrypted before being used. This requires the use of adequate passwords. The deletion of data takes place by means of secure processes. Data carriers out of use will be deleted and/or destroyed securely. For this purpose, a certified company will be instructed.

#### 5. Input Control ("Eingabekontrolle")

The use of own accounts for each employee allow specific identification.

#### 6. Order Control ("Auftragskontrolle")

The data protection officer carries out controls on a random basis within the company. Contracts with subcontractors regarding the processing of data on behalf contain corresponding rules which allow controls and instructions by EASY.

#### 7. Availability Control ("Verfügbarkeitskontrolle")

- All offices are equipped with a centralized fire alarm.
- The data center is equipped with an Uninterruptible Power Supply (UPS).
- The workstation computers are connected to a network with overvoltage protection.
- The server room is equipped with an air-conditioning system.
- The central backup server is located in another building section.
- Anti-virus protection software and organizational instructions in case of infections.

#### 8. Segregation Control ("Trennungskontrolle")

The data (e.g. documentations, etc.) are filed in separated directories. According to the data and the used software, corresponding segregation mechanisms are being used.

#### 9. Miscellaneous

An IT-security policy containing specific and comprehensive rules for the security of IT systems is available.

- As of 6/1/2017 -