Contract on Processing Personal Data on Behalf of a Controller

made and entered into by and between EASY SOFTWARE Deutschland GmbH Jakob-Funke-Platz 1, 45127 Essen, Germany 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 existing 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 the 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 third 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, the 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-organizational 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 this 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 the duration of this Agreement, employ that officer. The name of the data protection officer and the contact data can be obtained from the Processor's home page (www.easy-software.com).

3.6. The Processor shall support the Controller, taking the type of processing and the information available to him into account, when complying with the 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 organizational 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 routinely, 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, information 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 obligations 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. (6). 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 the 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, Jakob-Funke-Platz 1, 45127 Essen, Germany, Support and support of group IT services
  Subcontractors of EASY SOFTWARE AG:
  - Vodafone GmbH, Ferdinand-Braun-Platz 1, 40549 Düsseldorf, Germany, Support for Microsoft 365
  - SAP Deutschland SE & Co.KG, Rosenthaler Straße 30, 10178 Berlin, Germany, ERP system Sap ByD
  - KAMP Netzwerkdienste GmbH, Vestische Str. 89−91, 46117 Oberhausen, Germany, Colocation and hosting
  - TeamViewer Germany GmbH, Jahnstr. 30, 73037 Göppingen, Remote connection software
- OTRIS Software AG in Dortmund, Königswall 21, 44137 Dortmund, Germany, 3rd level support for Documents
- CTO Balzuweit GmbH, Lautlinger Weg 3, 70567 Stuttgart, Germany, 3rd level support for Capture Plus
- I.R.I.S. AG, Heusstraße 23, 52078 Aachen, 3rd Level Support for xTract
- friendWorks GmbH, Theresienplatz 31, 94315 Straubing, Consulting
- Heiko Fütterer, FocusOnIris, Karlstr. 5, 76287 Rheinstetten
- 7 Services Consulting GmbH, Schliemannstraße 6, 18211 Admannshagen-Bargeshagen
- Systec 2.0 GmbH, Am Neuen Werk 3, 33378 Rheda-Wiedenbrück

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 the company name
- Access to internal data centers has additional security. Only employees with the corresponding rights may enter this area.
- We use 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 certification 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 without 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 creation, 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 the 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.)

- For the separation of data, only systems are used that implement the separation either by tenant, logical separability based on data record identifiers, or by assigning roles with associated permissions.

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 28 of GDPR into account and thus suitability of the technical and organizational measures taken by them.
- Orders and, in conjunctions with them, contracts for processing on behalf of a controller are in writing.
- Contracts with subcontractors in third countries are precluded by the application of EU standard contractual clauses.
- 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 identifying 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)

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 initiating 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. Automatic 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.

Supplementary Annex 1 to the standard contract on processing of personal data on behalf of a controller (SaaS)

Purpose, nature and scope of data processing, type of data and group of people affected

Purpose of processing	▪ Providing EASY products as Software as a Service (SaaS) / Managed Application Hosting ▪ Running and maintaining EASY products as SaaS / Managed Application Hosting. ▪ Creating special configurations for EASY products as part of provision as SaaS / Managed Application Hosting
Type and scope of processing	▪ Accessing data via remote access ▪ Caching during remote access ▪ Displaying data via remote access ▪ Eliminating disruptions, and maintenance as part of SaaS / Managed Application Hosting ▪ Keeping implementation/customizing documentation or a project file regarding system, instance, tenant, client, or installation for the customer (= principal).
Type of data	▪ EASY provides the systems to the customer without personal data. The customer shall be responsible for GDPR-compliant data processing. He may only store and process personal data if permission is granted under the GDPR, German Federal Data Protection Act (Bundesdatenschutzgesetz, or BDSG), or any special law.
Group of people affected	▪ Controller's customers ▪ Controller's employees ▪ Controller's potential customers and prospects ▪ Controller's vendors ▪ Controller's sub-processors

Subcontractors approved in advance

- virtion GmbH, Südring 11, 33647 Bielefeld
  Deployment and operation of the server and data center infrastructure

Technical and organizational measures of virtion GmbH

Definition of responsibilities, as well as routine review and documentation of the related measures are laid down in the internal guidelines for document management, value management, and compliance of the certified Information Security Management System (ISMS) of virtion GmbH.

Annex Data Protection and Security Concept / Description of the technical and organizational measures in accordance with Art. 32, GDPR

This annex describes the technical and organizational measures of the data protection and security concept in accordance with Article 32 of the General Data Protection Regulation (GDPR) as part of the certified information security management system (ISMS) of virtion GmbH which are to be introduced and maintained in conjunction with the services provided or performed by virtion as part of processing on behalf of a controller.

§ 1 Pseudonymization

SUBJECT OF REGULATION:

Measures ensuring that personal data can no longer be attributed to a specific individual without additional information.

TECHNICAL AND ORGANIZATIONAL MEASURES:

Automatic pseudonymization or anonymization of IP addresses takes place as part of collecting access data to system services which are evaluated and analyzed for the purposes of maintaining information security, system security and system stability, as well as for the purposes of optimization and statistical collection of the use of services. Any further processing of personal data that allows useful pseudonymization does not take place. Regulations on appropriate identification and classification of data, the resulting procedure, the definition of responsibilities, and the routine review and documentation of the associated measures are laid down in the internal guidelines for document management, value management, and compliance of the certified information security management system (ISMS) of virtion GmbH.

§ 2 Encryption

SUBJECT OF REGULATION:

Measures taken to reduce the risk of physical, material or immaterial damage, or the risk of impairing the rights and freedoms of individuals affected through unauthorized disclosure of or access to data processed on behalf of a controller.

TECHNICAL AND ORGANIZATIONAL MEASURES:

Internal guidelines for cryptography as well as for encryption as part of access and access control, information transfer, and document management (certified according to ISO/IEC 27001 as part of the ISMS of virtion GmbH): these include regulations on technical and organizational measures for selecting cryptographic procedures and implementations; on the field of application of cryptographic systems (e.g. measured against security requirements), as well as regulations on key management (including regulations on the procedure for generation, separation, distribution, storage, access and absence management, validity period, and destruction of cryptographic keys). Routine reviews and documentation of the cryptographic procedures and systems used, the type of storage of the keys, and the respective validity period of the keys are carried out at least once a year as part of the continuous improvement process of the ISMS.

The internal guidelines for access control, information transfer, and document management, or value management contain regulations on technical and organizational measures to limit accessing internal systems via encrypted VPN access with two-factor authentication (including creation, disconnection of resulting access via VLANs, as well as role concepts, limited validity period, and disabling access), access to systems only via cryptographically encrypted connections (e.g. ssh), securing access to confidential data on workstations and mobile devices via the required full encryption of all data media (hard disks and all other data media), exclusively encrypted transmission of confidential information via the Internet, and exclusively encrypted storage of confidential data on physical media to be transported.

The internal incident management guideline regulates, among other things, the procedure in the event of the discovery of weak encryption procedures or systems, and contains detailed descriptions of measures, procedures and responsibilities for documenting and reporting corresponding information security weaknesses. The guideline and the resulting documentation requirements are part of routine (at least annual) internal and external audits of the ISMS of virtion GmbH.

§ 3 Confidentiality

Measures taken to reduce the risk of physical, material or immaterial damage or the risk that the rights and freedoms of individuals affected by unauthorized disclosure of or access to data processed on behalf of a principal.

Physical safety

SUBJECT OF REGULATION:

Measures taken to prevent unauthorized individuals from gaining access to the data processing, data storage, network, and telecommunications facilities (voice, data) used to process data on behalf of a controller.

TECHNICAL AND ORGANIZATIONAL MEASURES:

With regard to the technical and organizational measures for physical safety, in particular of the data processing systems and facilities in the data center of Telehouse Deutschland GmbH used by virtion GmbH via its service provider Filoo GmbH, reference is made to the existing security regulations for customers and external companies on behalf of the customer, which are part of the ISO27001 certification of the data center of Telehouse Deutschland GmbH, and can be viewed at virtion GmbH. These regulate, among other things, the purpose, scope of application, responsibilities, coordination of work, employee behavior, contact persons, plant security regulations, access regulations and controls, security regulations for video surveillance, fire protection, alerts, and building evacuation.

The concrete measures for access control to the data center include:

- Identity check at the reception including logging
- Electronic access control system including logging
- Guidelines for escorting and identifying of visitors
- Personalized key issuance to employees including logging
- Patrolling the premises by security service including logging
- Video surveillance of the building, inside and outside
- Intrusion alarm system including motion and contact detectors

Review and documentation of the technical and organizational measures for physical security of the data center are the subject of the internal guideline for vendor relations and thus a part of routine (at least annual) internal and external audits of the ISMS of virtion GmbH.

The internal guideline for access control (certified according to ISO/IEC 27001 as part of the ISMS of virtion GmbH) contains regulations on technical and organizational measures to secure access to the office location and to the employee offices or workplaces of virtion GmbH via locking systems, as well as on the individual and documented issuance of security keys and PIN codes to virtion GmbH employees; building security via door protection and motion detectors of the alarm system, as well as regulations on visits to the office location by external individuals.

Concrete measures for access control to the office location include:

- Identity check at the reception
- Electronic access control system including logging
- Guidelines for escorting visitors
- Personalized key issuance to employees including logging
- Intrusion alarm system including motion and contact detectors

Review and documentation of the technical and organizational measures for the physical safety of the office location is part of routine (at least annual) internal and external audits of the ISMS of virtion GmbH.

Authentication

SUBJECT OF REGULATION:
Measures taken to prevent data processing, data storage, network, and telecommunications facilities (voice, data) from being used by unauthorized third parties.

TECHNICAL AND ORGANIZATIONAL MEASURES:
The internal guideline for access control (certified according to ISO/IEC 27001 as part of the ISMS virtion GmbH) contains regulations on technical and organizational measures for access control systems, particularly encrypted VPN access with two-factor authentication, regulation of access control via granting and removing of user accounts for authenticating access to security critical and confidential systems; two-factor authentication using public-key procedures for access to servers, password management and the use of passwords; regulations on accessing to workstations by securing them with accounts using strong passwords; and the need for renewed login by automatic blocking, even if the user is only briefly out of the office. Verification and documentation of the technical and organizational measures for access control is part of routine (at least annual) internal and external audits of the ISMS of virtion GmbH.

Concrete measures for access control include:

- Master user/password database for access control of the customer's and contractor's employees
- Use of two-factor authentication for access control
- Access is only granted to the principal's and contractor's employees.
- Guidelines for the use of passwords (e.g. minimum length, characters used, etc.)
- Use of anti-malware software
- Use of firewalls

Permission concept

SUBJECT OF REGULATION:
Measures to ensure that persons authorized to use IT systems may only access data subject to their access permission. Data processed on behalf of a controller may not be read, copied, changed or removed when being processed.

TECHNICAL AND ORGANIZATIONAL MEASURES:
The internal guideline for access control (certified according to ISO/IEC 27001 as part of the ISMS of virtion GmbH) contains regulations on technical and organizational measures for access control systems, permission concepts, access controls via role concepts and role definitions; regulation of granting and removing access rights, securing access through cryptographic measures; regulations on user and rights management, automatic time limits for access, as well as regular checks on the correctness and documentation of accesses and granted permissions. Review and documentation of the technical and organizational measures for access control is part of routine (at least annual) internal and external audits of the ISMS of virtion GmbH.

Concrete access control measures include:

- Master user database including binding assignment of roles and permissions for the principal's and the contractor's employees
- Prevention of unauthorized access through regular security updates
- Logging of access to applications (in particular, when entering, modifying, or deleting data)
- Secure deletion of data media before reuse
- Safe disposal or destruction of storage media no longer needed or defective, including logging
- Use of document shredders for physical documents

Sharing of information

SUBJECT OF REGULATION:
Measures taken to ensure that data processed on behalf of a controller cannot be read, copied, modified or removed without permission during electronic transmission, or during transport or storage on data media.

TECHNICAL AND ORGANIZATIONAL MEASURES:
The internal guidelines for value management, access control, cryptography, network security, and information transmission contain regulations on technical and organizational measures for the exclusively encrypted transmission of confidential information via the Internet, on handling mobile storage solutions, as well as on full encryption of all data media (hard disks as well as all other data media), on transporting physical media, as well as on exclusively encrypted storage of confidential data on physical media to be transported.

Concrete measures to control data transfers include:

- Electronic transmission of confidential data is generally encrypted
- Storage of confidential data on physical media to be transported is generally encrypted

The regulations on resulting procedures, the definition of responsibilities and routine review and documentation of the associated measures are part of routine (at least annual) internal and external audits of the ISMS of virtion GmbH.

Deleting data

SUBJECT OF REGULATION:
Measures taken to keep personal data only for as long as is necessary for the purposes of processing.

TECHNICAL AND ORGANIZATIONAL MEASURES:
The internal guideline for value management contains regulations on technical and organizational measures for classification, labeling, and handling of confidential information as well as for storage, transmission and destruction of information. This includes secure destruction of data, documents and data media, as well as definition of responsibilities and procedures for the deletion of data and the disposal of physical media, and documentation of the deletion and secure disposal.

Concrete measures to delete data include:

- Data deletion in accordance with data protection regulations after the end of the contract
- Deletion or destruction of documents in accordance with data protection regulations after the end of the contract
- Deletion or destruction of data media in accordance with data protection regulations after the end of the contract

The regulations on resulting procedures, the definition of responsibilities and routine review and documentation of the associated measures are part of routine (at least annual) internal and external audits of the ISMS of virtion GmbH.

Client separation

SUBJECT OF REGULATION:
Measures taken to enable data collected for different purposes to be processed separately.

TECHNICAL AND ORGANIZATIONAL MEASURES:
The internal guidelines for internal organization, operational security and network security contain regulations on technical and organizational measures to separate customer systems and system environments to reduce the risk of unauthorized or unintentional access or changes to different system environments for development, integration, testing or production, as well as internal systems and customer systems and, where applicable, different systems of individual customers. This includes the definition of measures for the separation of networks through appropriate technical and organizational security measures, as well as the corresponding responsibilities and documentation specifications for administration and control of the underlying networks.

Concrete measures for separation control include:

- The processed data is stored physically or logically separated from other data.
- Backup is performed on logically and/or physically separate systems

The regulations on resulting procedures, the definition of responsibilities and routine review and documentation of the associated measures are part of routine (at least annual) internal and external audits of the ISMS of virtion GmbH.

§ 4 Integrity

Measures taken to reduce the risk of physical, material or immaterial damage or the risk that the rights and freedoms of individuals affected by accidental or unauthorized modification, or unlawful or negligent actions performed on data processed under contract.

Logging

SUBJECT OF REGULATION:
Measures taken to ensure subsequent verification and checking on whether and on whose behalf data has been processed, entered, modified in data processing systems, or removed from them.

TECHNICAL AND ORGANIZATIONAL MEASURES:
The internal guidelines on operational security contain regulations on technical and organizational measures for logging and monitoring events relating to information security and data protection; and for providing the corresponding documents and logs or evidence; for notification of undesired user activities, errors and exceptional states; for logging of remote access or remote access attempts; for preparation, storage, backup, protection and routine checking of the corresponding event logs; for protection of facilities; for logging and monitoring, as well as resulting recordings against manipulation or unauthorized access; and for logging activities of system administrators and system operators; moreover, on retention periods, archiving specifications, and access restrictions of the secured logging data.

Concrete measures for input control include:

- The data is entered or captured by the principal; responsibility for input control rests with the principal
- Logging of accessing applications and data (particularly when entering, modifying, or deleting data)

The regulations on the corresponding measures, the definition of responsibilities, and routine review and documentation of the associated measures are part of routine (at least annual) internal and external audits of the ISMS of virtion GmbH.

§ 5 Availability

Measures taken to reduce the risk of physical, material or immaterial damage or the risk of impairment of rights and freedoms, including through unlawful or negligent acts, for individuals as a result of the unavailability of data processed on behalf of a controller.

Ensuring availability

SUBJECT OF REGULATION:
Measures taken to protect data processed on behalf of the company against accidental or deliberate destruction or loss.

TECHNICAL AND ORGANIZATIONAL MEASURES:
With regard to the technical and organizational measures for the availability, in particular, of the data processing systems and equipment in the data center of Telehouse Deutschland GmbH used by virtion GmbH, reference is made to the existing measures which are part of the ISO27001 certification of the data center of Telehouse Deutschland GmbH, including access safeguards through structural measures; personnel measures such as identity checks at the reception including logging; electronic access control systems including logging, as well as guidelines for the escorting and identifying visitors; measures for resiliency such as redundant air conditioning systems, redundant UPS systems for uninterruptible power supply; fire protection concept including smoke detectors, automated extinguishing system for server rooms, as well as central monitoring and checking all operating

parameters of the data center by the data center operator or the operated systems and services by virtion GmbH including alerts.

Other security measures implemented by virtion GmbH include internal guidelines for operational security including regulations on technical and organizational measures and concepts for backup and recovery with at least daily backup of all relevant data, use of protective software (antivirus scanners, firewalls, encryption, spam filters); use of hard disk mirroring and RAID systems to increase reliability, redundant design of internal systems and resources; routinely reviewed emergency plans, routinely planned, performed and documented emergency tests to review the emergency plans, internal guidelines on business continuity management; routinely performed and documented business impact analyses as part of the risk management plan; routine analysis of threats and vulnerabilities and risk assessments as part of risk management as part of the information security management system.

Concrete measures for availability control include:

- Backup and recovery concept with at least daily backup of all relevant data
- Use of protective software (antivirus scanners, firewalls, encryption, spam filters)
- Use of hard disk mirroring / RAID systems
- Redundant air conditioning systems
- Redundant UPS systems for uninterruptible power supply
- Fire protection concept including smoke detectors
- Automated extinguishing system for server rooms
- Central monitoring and control of all operating parameters of the data center (data center operator), or the systems and services operated (virtion GmbH) including alerts

The regulations on resulting procedures, the definition of responsibilities and routine review and documentation of the associated measures are part of routine (at least annual) internal and external audits of the ISMS of virtion GmbH.

Earmarking

SUBJECT OF REGULATION:
Measures taken to ensure that personal data processed on behalf of a controller may only be processed in accordance with the instructions of the controller. This applies particularly to the deletion of data.

TECHNICAL AND ORGANIZATIONAL MEASURES:
Contractual regulations for processing on behalf of a controller with customers and vendors for the definition and specification of the data to be processed as part of the processing activities in the form of a list, of the application areas and responsibilities, of the duties of the principal controller (in particular, for regulating the authority of the customer to issue directives, to meet the requirements of data protection through suitable technical and organizational measures and to oblige individuals authorized to process data to maintain confidentiality); to deal with enquiries from individuals; to provide evidence, documentation requirements and to carry out audits by the customer, as well as the admissibility and regulation of the use of subcontractors as further order processors.

Concrete measures to control processing on behalf of a controller include:

- The principal (customer) and contractor have concluded written agreements for processing on behalf of a controller.
- The contractor may only use the principal's data in accordance with written agreements and directives from the principal. In particular, strict earmarking is agreed.
- The contractor is granted on-site control rights in the agreement on processing on behalf of a controller.
- Subcontractors are carefully selected and contractually bound in the same way as the processor is bound by the controller.

§ 6 Endurance

SUBJECT OF REGULATION:
Measures taken to reduce the risk of physical, material or immaterial damage or the risk of impairment of rights and freedoms, including by unlawful or negligent acts, to individuals through destruction, loss, modification or unauthorized disclosure of, or access to, data processed under contract due to system overloads or crashes.

TECHNICAL AND ORGANIZATIONAL MEASURES:
The internal policies on operational security, change management, incident management, business continuity management and risk management contain regulations on operational documentation and concepts, maintenance work, planning, implementation and documentation of changes; capacity management, separation of system environments; protection against malware; backup and recovery, logging and monitoring; system configuration and system hardening; responsibilities and procedures for reporting incidents; for evaluating, classifying, handling and documenting incidents; for reporting vulnerabilities including impact on information security; for planning, implementing and reviewing emergency management and the associated emergency plans; for redundant design of internal systems and resources; for planning, executing and documenting emergency tests as preventive measures; for routine review of the correctness of the measures from the emergency plans, and for routine analysis of threats and vulnerabilities as part of risk management.

The regulations on the corresponding measures, the definition of responsibilities and routine review and documentation of the associated measures are part of routine (at least annual) internal and external audits of the ISMS of virtion GmbH.

§ 7 Techniques for restoring the availability of personal data following a physical or technical incident

SUBJECT OF REGULATION:
Measures taken to reduce the risk of physical, material or immaterial damage or the risk that rights and freedoms may be impaired, including by unlawful or negligent actions, to individuals through the destruction, loss, modification or unauthorized disclosure of, or access to, data processed on behalf of a controller, as a result of a physical or technical incident.

TECHNICAL AND ORGANIZATIONAL MEASURES:
The internal guidelines for operational security, incident management and business continuity management contain regulations on the separation of system environments; on data backup and data recovery; on responsibilities and procedures for reporting information security incidents; on evaluating, classifying, handling and documenting information security incidents; on the analysis and use of knowledge gained from information security incidents; on the reporting of weak points impacting information security; on redundant design of internal systems and resources; on planning, implementing and reviewing emergency management and the associated emergency plans as part of an emergency manual; for planning, executing and documenting emergency tests as preventive measures to routinely review the

correctness of the measures from the emergency plans, as well as for training in emergency situations and for the protection of critical systems, information and business processes from the impact of major failures of information systems and infrastructures and recovery within a reasonable period of time as part of the business continuity management of virtion GmbH.

The regulations on the corresponding measures, the definition of responsibilities and routine review and documentation of the associated measures are part of routine (at least annual) internal and external audits of the ISMS of virtion GmbH.

§ 8 Techniques for regular review, assessment and evaluation of the effectiveness of technical and organizational measures

SUBJECT OF REGULATION:

Presentation of the techniques for routine review, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure the security of processing.

TECHNICAL AND ORGANIZATIONAL MEASURES:

The internal guidelines for risk management, internal audits, management reviews, personnel security, and measuring the effectiveness of the ISMS contain regulations on routine analysis of threats and weaknesses, as well as risk assessments as part of risk management; for routine planning, executing and documenting internal audits of the ISMS; on routine planning, carrying out and documenting management reviews to ensure that the ISMS complies with the standards; for fulfilling the information security objectives of virtion GmbH; for management commitment; for securing resources for the operation of the ISMS, as well as for continuous improvement of the ISMS, routine training; and for ensuring the competence and awareness of the employees as well as routine review and documentation of the effectiveness of the measures of the ISMS and, if applicable, of the measures taken, as well as any resulting measures as part of the continuous improvement of the ISMS.

The regulations on the corresponding measures, the definition of responsibilities as well as routine review and documentation of the associated measures are part of routine (at least annual) internal and external audits of the ISMS of virtion GmbH, certified according to ISO 27001.

Additional technical and organizational measures (EASY Cloud)

The following measures should be considered to be in addition to the measures from the standard contract for processing on behalf of a controller; they represent cloud-specific supplements.

ACCESS CONTROL:
- In addition, the respective access rules of virtion GmbH apply.

ACCESS CONTROL / USER CONTROL:
- Administrative access to the cloud systems is only possible via cryptographically secured connections.
- Personalized administrative credentials are used for each cloud system.
- Passwords must have a minimum length of 12 characters, and be sufficiently complex.
- Administrative access is additionally secured by using a VPN.

ACCESS CONTROL / STORAGE CONTROL / DISK CONTROL:
- The virtual machines are separated from each other on the network.
- Possible scripting capabilities in the products are disabled for the customer. Scripts can only be implemented by EASY employees.
- Basically, customers have no or only limited administration options at application level via a Web interface.

SEPARATION RULE / SEPARABILITY:
- The data is separated by clients/instances.

ENCRYPTION:
- Administrative access to the cloud systems is only possible via cryptographically secured connections.
- For the customer, access is only possible via HTTPS secured connections.

TRANSPORT CONTROL / TRANSMISSION CONTROL (TRANSFER CONTROL):
- Use of a reverse proxy to filter non-permissible requests.
- Enforce HTTPS on all requests.

Availability, endurance / resiliency, recoverability
(i.e. data is available when it is needed)

AVAILABILITY CONTROL:
(ensures that personal data is protected against destruction or loss, e.g. by fire protection measures, etc.)

- See virtion measures

ENDURANCE (WITHIN THE MEANING OF RESILIENCY):
(ensures that IT systems are resilient to attacks)

- Use of a firewall.
- Use of a reverse proxy.

RESTORABILITY:
(ensures that systems used can be restored in the event of a failure)

- The data is backed up every day.