

Agreement on Commissioned Data Processing

Last Update: September 2023

This Agreement on Commissioned Data Processing between the user of OSDi LiveGuide Service (“Controller”) and Fette Compacting GmbH (“Processor”) that regulates the data processing. **BY DOWNLOADING, INSTALLING AND USING THE SOFTWARE YOU CONSENT TO THESE CONDITIONS. IF YOU DO NOT CONSENT TO THESE CONTRACTUAL PROVISIONS, YOU ARE NOT ENTITLED TO USE THE SOFTWARE.**

§ 1 Subject of the Agreement and Term

- (1) The Processor performs services for the Controller as described in Appendix 1. Appendix 1 details the subject-matter, type and purpose of processing, the types of data and categories of data subjects.
- (2) This Agreement shall – unless otherwise agreed – become effective after downloading, installing and using the app and shall apply as long as the Processor processes personal data on behalf of the Controller.

§ 2 Instructions of the Controller

- (1) The Controller is responsible for compliance with the relevant data protection provisions, in particular for the admissibility of the data processing and for safeguarding the data subjects' statutory rights, stipulated by the GDPR. Statutory or contractual liability provisions shall remain unaffected.
- (2) The Processor processes the personal data disclosed by the Controller solely under the instructions of the Controller and within the scope of the agreed services/stipulations. Data must only be corrected, erased or blocked subject the Controller's instructions.
- (3) Unless processing of certain personal data is required by law of the European Union or a Member State to which the Processor is subject, the Processor must only process data under the Controller's instruction. In such a case, the Processor shall inform the Controller of that legal requirement prior to processing, unless that law prohibits such information on important grounds of public interest.
- (4) The Controller's instructions require no specific form. Verbal instructions must be documented by the Controller. Instructions must be given in writing or in text form, if the Processor requires it.
- (5) If the Processor believes that an instruction given by the Controller infringes upon data protection laws, he must inform the Controller of this without undue delay.

§ 3 Technical and Organizational Measures

- (1) The Processor undertakes to employ adequate technical and organizational security measures for the data processing and to document them in Appendix 3 of this Agreement. These security measures should be appropriate to the risks involved with the specific personal data processing operations.
- (2) The measures that have been taken can be adapted to future technical and organizational developments. The Processor may only carry out these adaptations, if they satisfy at least the previous level of security. Where no other regulations exist, the Processor must only inform the Controller of substantial changes.
- (3) The Processor shall support the Controller to comply with all legal obligations as far as the technical and organizational measures are concerned. The Processor shall, upon request, cooperate in creating and maintaining the Controller's record of processing activities. The Processor shall cooperate with the creation of a data protection impact assessment and if necessary with prior consultations with supervisory authorities. Upon request, the Processor shall disclose the required information and documents to the Controller.

§ 4 Obligations of the Processor

- (1) The Processor confirms that he is aware of the relevant data protection regulations. The Processor's internal operating procedures shall comply with the specific requirements of an effective data protection management.
- (2) The Processor guarantees that he has implemented appropriate technical and organizational measures, in a way that the processing is in compliance with the requirements of data protection law and the rights of data subjects.
- (3) The Processor warrants and undertakes that all employees involved in the personal data processing procedures are familiar with the relevant data protection regulations. The Processor assures that those employees are bound to maintain confidentiality, or are subject to an adequate legal obligation of secrecy. The Processor shall monitor compliance with the applicable data protection regulations.
- (4) The Processor may only access the Controller's personal data if it is necessary for the purposes of carrying out the data processing.
- (5) Insofar as it is legally required, the Processor shall appoint a Data Protection Officer. The Processor's Data Protection Officer's contact details are to be shared with the Controller for the purposes of making direct contact.
- (6) The Processor may only process personal data provided to him exclusively in the territory of the Federal Republic of Germany or in a Member State of the European Union. Processing personal data in a third country must meet the relevant legal requirements.
- (7) The Processor supports the Controller with appropriate technical and organizational measures to ensure that the Controller can fulfill his obligations to respond to requests for exercising the data subject's rights, e.g. the right to information, the right to rectification and to erasure, the right to restriction of processing, to data portability and to object. The Processor will nominate a contact person who will support the Controller in the fulfillment of legal obligations to provide information in connection with the data processing, and will share this person's contact details with the Controller without undue delay. The Processor shall support the Controller, insofar as the Controller is subject to information obligations in the event of a data breach. Information may only be given to data subjects or to third parties with the prior instruction of the Controller. If a data subject exercises his or her data subject's rights in respect to the Processor, the Processor shall forward this request to the Controller without undue delay.

§ 5 Authority to Conclude a Subprocessing Agreement

- (1) The Processor may only assign Subprocessors, after informing the Controller of every intended change in relation to the addition of or replacement of a Subprocessor, whereby the Controller has the opportunity to veto the intended change. The controller may only veto with good cause.
- (2) A relationship shall be regarded as that of a Subprocessor when the Processor commissions other Processors in part or in whole for services agreed upon in this contract. Ancillary services that are provided to and on behalf of the Processor by third party service providers and that are determined to support the Processor to execute the assignment services, shall not be regarded as Subprocessors within the meaning of this Agreement. Such services may include, for example, provision of telecommunication services or facility management. However, the Processor is obliged to guarantee the protection and the security of the Controller's data in respect to third party service providers, and to ensure appropriate and legally compliant contractual agreements and supervisory measures are in place.
- (3) A Subprocessor may only have access to the data once the Processor has ensured, by means of a written contract, that the regulations of this contract are also binding against the Subprocessor, and in particular adequate guarantees are provided that appropriate technical and organizational measures are carried out in a way so that the processing is compliant with data protection regulations.
- (4) The commissioning of Subprocessors listed in Appendix 2 of this Agreement at the time of signature are deemed to be approved, provided that the requirements of § 5 Para. 3 of this Agreement are implemented.
- (5) If the controller or a Subprocessor agree to the assignment of (further) subprocessors in third countries, the following provisions shall apply, unless an adequate level of data protection at the respective subprocessor is otherwise ensured.

A data transfer to the third country may only take place if, at the time of retaining the subprocessing, at the latest before the first data transfer, the Standard Contractual Clauses for the transfer of personal data to processors in third countries in accordance with Commission Decision 2010/87/EU have been concluded with the subprocessor.

By signing this Agreement, the processor shall be obliged and authorized to the extent necessary for this purpose, to conclude the Standard Contractual Clauses 2010/87/EU with the third country subprocessor in the name and on behalf of the controller.

For the purposes of the Standard Contractual Clauses 2018/87/EU, the controller is deemed to be the "data exporter" and the subprocessor is deemed to be the "data importer".

Since the subprocessor is assigned by the processor, the processor is primarily responsible vis-à-vis the controller (data exporter) for ensuring that the subprocessor (data importer) fulfills its obligations under the Standard Contractual Clauses 2010/87/EU. For this purpose, the processor shall have corresponding derived control obligations vis-à-vis the data importer and may exercise the power of control of the data exporter described in the Standard Contractual Clauses 2010/87/EU. The controller remains obliged to monitor the exercise of the power of control and may also exercise this itself at any time vis-à-vis the subprocessor. The provisions of the Standard Contractual Clauses 2010/87/EU shall, with this proviso, also apply to the processor, who shall accede to the contract between the controller and the subprocessor.

The processor is obliged to provide the controller with a copy of the signed standard contractual clauses in a timely manner and without further request.

§ 6 Controller's Right of Inspection

The Processor agrees that the Controller or a person authorized by him shall be entitled to monitor compliance with the data protection provisions and the contractual agreements to the extent necessary, in particular by gathering information and requests for relevant documents, the inspection of data-processing programs or accessing the working rooms of the Processor during the designated office hours after prior notice. Proof of proper data processing can also be provided by appropriate and valid certificates for IT security (e.g. IT-Grundschutz, ISO 27001), provided that the specific subject of certification applies to the commissioned data processing in the specific case. However, presenting a relevant certificate does not replace the Processor's duty to document the safety measures within the meaning of § 3 of this Agreement.

§ 7 Obligation to Report Data Protection Violations by the Processor

The Processor shall notify the Controller without undue delay about any disruption in operation which implicates menace to personal data provided by the Controller, as well as of any suspicion of data protection infringements concerning personal data provided by the Controller. The same applies if the Processor discovers that his security measures do not satisfy legal requirements. The Processor is aware that the Controller is obligated to document all breaches of the security of personal data and, where necessary, to inform the supervisory authority and/or the data subjects. The Processor will report breaches to the Controller without undue delay and will provide, at a minimum, the following information:

- a) A description of the nature of the breach, the categories and approximate number of data subjects and personal data records concerned,
- b) Name and contact details of a contact person for further information,
- c) A description of the likely consequences of the breach, and
- d) A description of the measures taken for the remedy or mitigation of the breach.

§ 8 Termination of the Agreement

- (1) On termination or expiration of this Agreement the Processor shall return or erase all personal data, by choice of the Controller, provided there is no statutory duty to preserve records for retention periods set by law or agreement.
- (2) The Controller can terminate the contractual relationship without notice if the Processor gravely violates this Agreement or the legal provisions of data protection and the Controller can therefore not reasonably be expected to continue the data processing until the expiry of the notice period or the agreed termination of Agreement.

§ 9 Final Provisions

- (1) In case any of the Controller's property rights are at risk in the office premises of the Processor due to measures taken by third parties (e.g. through seizures or confiscation), insolvency proceedings or any other events, the Processor shall promptly inform the Controller hereof. The Processor waives the right of lien in respect to storage media and datasets.
- (2) Any and all modifications, amendments and supplements to this Agreement must be in writing and can also be made in an electronic format.
- (3) Should a provision of this Agreement become unenforceable, that shall not affect the validity or enforceability of any other provision of this Agreement.

Appendix 1: List of Contracted Services and contact details of the data protection officers

Subject-matter of the Processing	Services in connection with OSDI LiveGuide Service ("Service")
Nature and Purpose of the Processing	The software is an augmented reality remote support software via browser or application. The software allows the client to communicate directly (chat) with the contractor, its employees and/or third parties, exchange documents and/or images and/or hold discussions in an augmented reality-based video conference.
Type of Personal Data	Types of personal data concerned: <ul style="list-style-type: none"> • Personal master data <ul style="list-style-type: none"> ◦ surname, first name, company ◦ gender • communications data (e.g. phonenumber, e-mail) • contract master data • customer history • communication content • video, pictures
Categories of Data Subjects	Customers, interested parties, employees of the customer, contact persons, third party invited by customer to use the service.

Name and contact details of the controller's data protection officer (if designated)	
Name and contact details of the processor's data protection officer (if designated)	Datenschutz nord GmbH Sechslingspforte 2 22087 Hamburg Germany

Appendix 2: List of Deployed Subprocessors including the Processing Sites

Subprocessor (Name, legal status, place of business)	Processing site	Type of service
ADTANCE GmbH & Co. KG, Hauptstraße Nord 55, 69483 Wald- Michelbach	Falkenstein, Nürnberg, Frankfurt (Germany)	Maintenance, provision of application services

Appendix 3: Technical and Organizational Measures

A. Measures for the assurance of confidentiality and integrity

1.	Measures of access control related to the server rooms
1.0	Are personal data stored on servers that are operated by you? <input type="checkbox"/> yes <input checked="" type="checkbox"/> no
	If 1.0 no: In this case the further questions under A1 <u>do not</u> need to be answered. Continue to A2. Furthermore, questions B1 and B2 also do not require an answer.
1.1	Location of the server room / data center (DC) Frankfurt am Main
1.2	Are the personal data stored in more than one server location / data center? (i.e. on back up servers, cloud services)? <input type="checkbox"/> yes <input checked="" type="checkbox"/> no
1.3	If 1.2 yes: Please also fill out the appropriate details of the further locations. Further server locations:
1.4	Does the following information regarding access control measures apply to all server locations / data centers in use? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
1.5	If 1.4 no: Please answer questions 1.6 to 1.21 and section B for further locations.
1.6	Is the server room windowless? DC 1 <input checked="" type="checkbox"/> yes <input type="checkbox"/> no DC 2 <input type="checkbox"/> yes <input type="checkbox"/> no
1.7	If 1.6 no: How are the windows protected from burglary? <input type="checkbox"/> barred <input type="checkbox"/> alarmed <input type="checkbox"/> lockable <input type="checkbox"/> not at all <input type="checkbox"/> Other: Please specify
1.8	Is the server room secured by an alarm system? DC1 <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
1.9	If 1.8 yes: Who is informed if the alarm system is triggered? Multiple answers possible! <input type="checkbox"/> Commissioned security firm <input type="checkbox"/> Administrator <input checked="" type="checkbox"/> IT manager <input checked="" type="checkbox"/> Other
1.10	Is the server room under video surveillance? <input type="checkbox"/> yes, without image recording <input checked="" type="checkbox"/> yes, with image recording <input type="checkbox"/> no
1.11	If 1.10 yes, with image recording: How long is the video footage stored? 180 days
1.12	How many people have access to the server room and which functions do they have? Number of persons Role in the company:
1.13	Is there an electronic lock system in place in the server room? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no, there is a mechanical lock

1.14	If 1.13 yes: Which entry technology is in use? Multiple answers possible! <input checked="" type="checkbox"/> RFID <input checked="" type="checkbox"/> PIN <input checked="" type="checkbox"/> Biometrics <input type="checkbox"/> Other: please specify
1.15	If 1.13 yes: Are access rights assigned individually? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
1.16	If 1.13 yes: Will accesses to the server room be logged in the access system? <input checked="" type="checkbox"/> yes, successful as well as unsuccessful attempts <input type="checkbox"/> yes, but only successful accesses <input type="checkbox"/> yes, but only unsuccessful attempts <input type="checkbox"/> no, the lock will only be released or not.
1.17	If 1.16 is yes: For how long will access data be stored before erasure? Please insert value in days days
1.18	If 1.13 no: how many keys to the server room exist, where are they stored and who distributes them? Number of keys: Number of keys Storage location: Insert storage location Person responsible for distributing keys: please specify
1.19	What is the access door to the server room made of? <input checked="" type="checkbox"/> Steel / Metal <input type="checkbox"/> Other material
1.20	Is the server room being used for other purposes besides its actual function? <input type="checkbox"/> yes <input checked="" type="checkbox"/> no
1.21	If 1.20 yes: What else is kept in the server room? <input type="checkbox"/> Telephone system <input type="checkbox"/> Storage of stationery <input type="checkbox"/> Storage of files <input type="checkbox"/> Archive <input type="checkbox"/> Storage of IT equipment <input type="checkbox"/> Other: please specify
	In your opinion, are the documented measures appropriate, given the state of the art, implementation costs, nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of the data subject, such that an appropriate standard of protection is guaranteed? <input checked="" type="checkbox"/> Appropriate <input type="checkbox"/> Appropriate with reservations <input type="checkbox"/> Inappropriate
2.	Access control measures to the office rooms
2.1	Location(s) of the client workstations, from which personal data are accessed: all German locations of LMT Group
2.2	Is there a porter service / a constantly occupied lobby area to the building / to the office? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
2.3	Is a visitor's book implemented? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
2.4	Is the building or is the office protected by a burglar alarm? <input type="checkbox"/> yes <input checked="" type="checkbox"/> no
2.5	If 2.4 yes: Who is informed if the alarm system is triggered? Multiple answers possible! <input type="checkbox"/> Commissioned security firm <input type="checkbox"/> Administrator <input type="checkbox"/> IT manager <input type="checkbox"/> Other: please specify
2.6	Is the office building or its entrances under video surveillance? <input checked="" type="checkbox"/> yes, without image recording <input type="checkbox"/> yes, with image recording <input type="checkbox"/> no
2.7	If 2.6 yes, with image recording: For how long is the video footage stored? 30 days

2.8	<p>Are the building / office rooms secured with an electronic lock system?</p> <p><input type="checkbox"/> yes, building and office rooms are electronically locked</p> <p><input checked="" type="checkbox"/> yes, but only the building, not the entrance to the office or to the story that the office is on and only between 4:30pm and 7:00am.</p> <p><input type="checkbox"/> yes, but only the entrance to the office / the story that the office is on, not the entire building</p> <p><input type="checkbox"/> no</p>
2.9	<p>If 2.8 yes: Which entry technology is in use? Multiple answers possible!</p> <p><input checked="" type="checkbox"/> RFID <input type="checkbox"/> PIN <input type="checkbox"/> Biometrics <input type="checkbox"/> Other: <input type="text" value="please specify"/></p>
2.10	<p>If 2.8 yes: Are access rights assigned individually?</p> <p><input checked="" type="checkbox"/> yes <input type="checkbox"/> no</p>
2.11	<p>If 2.8 yes: Will accesses to the server room be logged in the access system?</p> <p><input checked="" type="checkbox"/> yes, successful as well as unsuccessful attempts</p> <p><input type="checkbox"/> yes, but only successful accesses</p> <p><input type="checkbox"/> yes, but only unsuccessful attempts</p> <p><input type="checkbox"/> no, the lock will only be released or not.</p>
2.12	<p>If 2.11 yes: For how long will access data be stored before deletion?</p> <p>30 days</p>
2.13	<p>If 2.11 yes: Are the records regularly assessed?</p> <p><input type="checkbox"/> yes <input checked="" type="checkbox"/> no, but assessment would be possible if required</p>
2.14	<p>Is there a mechanical lock for the building / office rooms?</p> <p><input checked="" type="checkbox"/> yes <input type="checkbox"/> no</p>
2.15	<p>If 2.14 yes: Is the key distribution recorded, who distributes them?</p> <p><input checked="" type="checkbox"/> yes <input type="checkbox"/> no Responsible person: facility management</p>
2.16	<p>Are there official access regulations for visitors to the premises?</p> <p><input type="checkbox"/> no</p> <p><input checked="" type="checkbox"/> yes, visitors will be received at the entrance / reception by the contact person and must be accompanied at all times</p>
	<p>In your opinion, are the documented measures appropriate, given the state of the art, implementation costs, nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of the data subject, such that an appropriate standard of protection is guaranteed?</p> <p><input checked="" type="checkbox"/> Appropriate <input type="checkbox"/> Appropriate with limitations <input type="checkbox"/> Inappropriate</p>
3	Access control measures to the system
3.1	<p>Is there a process for the distribution of access information (e.g. user names) and access rights for newly instated / removal of access information for departing employees, or for organizational changes?</p> <p><input checked="" type="checkbox"/> Defined distribution process</p> <p><input type="checkbox"/> No defined distribution process, on demand</p> <p><input type="checkbox"/> Other: <input type="text" value="please specify"/></p>
3.2	<p>Is assigning or changing the access information recorded?</p> <p><input checked="" type="checkbox"/> yes <input type="checkbox"/> no</p>

3.3	Do employees log in via an individual authorization in the central directory service? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
3.4	Are binding password parameters in operation? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
3.5	What measures are taken when a password is lost, forgotten or compromised? <input checked="" type="checkbox"/> Admin issues a new initial password <input type="checkbox"/> None
3.6	How does authentication occur by remote accesses? <input type="checkbox"/> Token <input checked="" type="checkbox"/> VPN-Certificate <input type="checkbox"/> Password
3.7	Are the systems that process personal data secured by a firewall? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
3.8	If 3.7 yes: Is the firewall updated regularly? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
	In your opinion, are the documented measures appropriate, given the state of the art, implementation costs, nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of the data subject, such that an appropriate standard of protection is guaranteed? <input checked="" type="checkbox"/> Appropriate <input type="checkbox"/> Appropriate with limitations <input type="checkbox"/> Inappropriate
4	Measures for the assurance of paper documents, mobile data carriers and mobile devices
4.1	How are redundant documents containing personal information (e.g. printouts / files / correspondence) disposed of? <input type="checkbox"/> wastepaper / residual waste <input checked="" type="checkbox"/> shredders, the use of which is advised <input checked="" type="checkbox"/> Documents are stored in securely locked disposal bin and sent to certified disposal service provider for destruction. <input type="checkbox"/> Other: please specify
4.2	How are redundant data media containing personal information (e.g. USB sticks, hard disks) disposed of? <input type="checkbox"/> physical destruction by internal IT department <input checked="" type="checkbox"/> physical destruction by an external service provider <input type="checkbox"/> Deletion of data by please insert number overwrites <input type="checkbox"/> Other: please specify
4.3	Are mobile data carriers permitted (e.g. USB sticks)? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
4.4	Can employees use their own personal data carriers (e.g. personal USB sticks)? <input type="checkbox"/> in general, yes <input type="checkbox"/> yes, but only after authorization and assessment of the storage device by the IT <input checked="" type="checkbox"/> no, all necessary storage devices are issued by the company
4.5	Do employees process personal data on their own private devices (bring your own device)? <input type="checkbox"/> yes <input checked="" type="checkbox"/> no

	<p>In your opinion, are the documented measures appropriate, , given the state of the art, implementation costs, nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of the data subject, such that an appropriate standard of protection is guaranteed?</p> <p> <input checked="" type="checkbox"/> Appropriate <input type="checkbox"/> Appropriate with limitations <input type="checkbox"/> Inappropriate </p>
5	Measures for secure data transfer
5.1	<p>In which way are data transferred?</p> <p> <input checked="" type="checkbox"/> data transfer only per mpls <input checked="" type="checkbox"/> individually coded <input type="checkbox"/> an encrypted file as a mail attachment <input type="checkbox"/> via PGP/SMime <input checked="" type="checkbox"/> via an encrypted data carrier <input type="checkbox"/> via VPN <input checked="" type="checkbox"/> via https/TLS <input type="checkbox"/> via SFTP <input checked="" type="checkbox"/> Other: encrypted documents </p>
5.2	<p>Who administers the keys / certificates?</p> <p> <input type="checkbox"/> Administrator themselves <input checked="" type="checkbox"/> Internal IT <input type="checkbox"/> External service provider </p>
5.3	<p>Are data transfers documented?</p> <p> <input type="checkbox"/> yes <input checked="" type="checkbox"/> no </p>
5.4	<p>If 5.3 yes: How long can recorded data be stored?</p> <p>please insert value in days days</p>
5.5	<p>If 5.3 yes: Are records regularly assessed?</p> <p> <input type="checkbox"/> yes <input type="checkbox"/> no, but an assessment would be possible if required </p>
	<p>In your opinion, are the documented measures appropriate, given the state of the art, implementation costs, nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of the data subject, such that an appropriate standard of protection is guaranteed?</p> <p> <input checked="" type="checkbox"/> Appropriate <input type="checkbox"/> Appropriate with reservations <input type="checkbox"/> Inappropriate </p>

B. Measures for the assurance of availability

1.	Server rooms
1.1	Does the server room have a fireproof / fire-resisting access door? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
1.2	Is the server room fitted with smoke detectors? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
1.3	Is the server room connected to a fire alarm control panel? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
1.4	Is the server room fitted with extinguishing systems? Multiple answers possible! <input checked="" type="checkbox"/> yes, CO2 extinguishers <input checked="" type="checkbox"/> yes, Halon / Argon extinguishing system <input checked="" type="checkbox"/> others: fire extinguisher
1.5	What are the external walls of the server rooms made of? <input checked="" type="checkbox"/> solid wall (e.g. concrete) <input type="checkbox"/> lightweight construction <input type="checkbox"/> Fireproof wall (e.g. F90)
1.6	Is the server room air-conditioned? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
1.7	Does the server room have an uninterruptible power supply (UPS)? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
1.8	Is the power supply to the server room also ensured via a diesel-powered generator? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
1.9	Are the functionalities in 1.2, 1.3, 1.4, 1.6, 1.7 and 1.8, where present, regularly tested? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
	In your opinion, are the documented measures appropriate, given the state of the art, implementation costs, nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of the data subject, such that an appropriate standard of protection is guaranteed? <input checked="" type="checkbox"/> Appropriate <input type="checkbox"/> Appropriate with reservations <input type="checkbox"/> Inappropriate
2	Backup- and emergency concepts, virus protection
2.1	Is a backup concept in place? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
2.2	Is the functionality of the backup creation regularly tested? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no

2.3	How frequently are backups from systems which store personal data created? <input type="checkbox"/> Real time <input checked="" type="checkbox"/> Daily <input type="checkbox"/> One to three times a week <input type="checkbox"/> Other: Please specify
2.4	On what storage devices are the backups stored? <input checked="" type="checkbox"/> Second redundant server <input type="checkbox"/> Backup Tapes <input checked="" type="checkbox"/> Hard drives <input type="checkbox"/> Other: please specify
2.5	Where are the backups stored? <input checked="" type="checkbox"/> Second redundant server at a separate location <input type="checkbox"/> In a safe which is fire resistant and data carrier- and document safe <input type="checkbox"/> in a normal safe <input type="checkbox"/> bank drawer <input type="checkbox"/> lockable drawer / filing cabinet <input type="checkbox"/> in a server room <input type="checkbox"/> private household <input type="checkbox"/> Other: please insert storage location
2.6	Regarding 2.5: Where backups are being transported: how does this occur? <input type="checkbox"/> Taken by an IT employee / Management / Secretary <input type="checkbox"/> Collection by a third party (i.e. bank employee / surveillance company) <input checked="" type="checkbox"/> Other:
2.7	Are the backups encrypted? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
2.8	Is the backup storage location in a separate fire area from the primary server? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
2.9	Is there a process for software or patch- management? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no <input type="checkbox"/> Process is in place, but is not documented
2.10	If 2.9 yes, who is responsible for the software or patch- management? <input type="checkbox"/> Administrator themselves <input checked="" type="checkbox"/> Internal IT <input checked="" type="checkbox"/> External service provider
2.11	Is an emergency concept in place (emergency measures in the event of an emergency, hardware defects, fire, data loss, etc.)? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no
2.12	Are the IT systems technologically protected from data loss / unauthorized data access? Yes, via an always updated <input checked="" type="checkbox"/> Virus protection <input checked="" type="checkbox"/> Anti-Spyware <input checked="" type="checkbox"/> Spam filter
2.13	If 2.12 yes, who is responsible for the updated virus protection, spyware and spam filter? <input checked="" type="checkbox"/> Administrator themselves <input type="checkbox"/> Internal IT <input checked="" type="checkbox"/> External service provider
	In your opinion, are the documented measures appropriate, given the state of the art, implementation costs, nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of the data subject, such that an appropriate standard of protection is guaranteed? <input checked="" type="checkbox"/> Appropriate <input type="checkbox"/> Appropriate with reservations <input type="checkbox"/> Inappropriate
3	Network connection
3.1	Does the company have a redundant internet connection? <input checked="" type="checkbox"/> yes <input type="checkbox"/> no

3.2	<p>Are the individual locations of the company connected via a redundant connection?</p> <p><input checked="" type="checkbox"/> yes <input type="checkbox"/> no</p>
3.3	<p>Who is responsible for the network connection of the company?</p> <p><input type="checkbox"/> Internal IT <input checked="" type="checkbox"/> External service provider</p>
	<p>In your opinion, are the documented measures appropriate, given the state of the art, implementation costs, nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of the data subject, such that an appropriate standard of protection is guaranteed?</p> <p><input checked="" type="checkbox"/> Appropriate <input type="checkbox"/> Appropriate with reservations <input type="checkbox"/> Inappropriate</p>