Agreement on Commissioned Data Processing between

– hereinafter “Controller”–

and

dbh Logistics IT AG
Martinistraße 47-49
28195 Bremen
– hereinafter “Processor”–

§ 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 it has been signed by both parties 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 adaptions, 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 Processer 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 Processer 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 always requires prior written approval by the Controller and 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 toinformation, 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 with the prior written approval of the Controller.

(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 agrees to the assignment of 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.

For this purpose, the processor shall be obliged and authorized to the extent necessary by signing this Agreement, 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 subcprocessor is deemed to be the "data importer".

Since the subprocessor is assigned by the processor, the processor is primarily responsible vis-a-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.

(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.

Place Date

Controller

_____________________________ _____________________________

Authorised Signature Name and function

Bremen,

dbh Logistics IT AG
Processor

_____________________________ _____________________________

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

Subject-matter of the Processing	Content of the data processing is evident from the respective contract with the orderer.
Nature and Purpose of the Processing	Purpose of the tasks of the Processor are described in the main contract.
Type of Personal Data	Adress data, personal data, contract data, payment data, planning and review process data.
Categories of Data Subjects	Employees, clients, interested parties, suppliers, resellers, cooperation partner, contact person.

The controller`s data protection officer (if designated)	
The processor`s data protection officer (if designated)	Mr. Dr. Uwe Schläger datenschutz nord GmbH Konsul-Schmidt-Straße 88 28217 Bremen Tel.: 0421 69 66 32 0 Fax: 0421 69 66 32 11 office@datenschutz-nord.de

Appendix 2: List of Deployed Subprocessors including the Processing Sites

Subprocessor (Name, legal status, place of business)	Processing site	Type of service
Bremen Briteline GmbH Wiener Str. 5 28359 Bremen	Bremen, Germany	Hosting.

dbh stores and hosts customer data solely in the above mentioned data centers in Bremen, Germany.

Appendix 3: Technical and Organizational Measures

(Please fill out the attached checklist, or clarify whether an existing IT-security concept can be incorporated into the Agreement.)

A. Measures for the assurance of confidentiality and integrity

1.	Measures of access control related to the server rooms
1.0	Is personal data under the controller's responsibility stored on servers that are operated by you or one of your service providers, if any? ☒ yes ☐ no
	If 1.0 no: In this case the further questions under A1 do not 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) Martinistr. 47-49, 28195 Bremen
1.2	Is personal data stored in more than one server location / data center? (i.e. on back up servers, cloud services)? ☒ yes ☐ no
1.3	If 1.2 yes: Please also fill out the appropriate details of the further locations. Further server locations: Bremen Briteline GmbH, Wiener Str. 5, 28359 Bremen
1.4	Does the following information regarding access control measures apply to all server locations / data centers in use? ☒ yes ☐ no
1.5	If the answer to 1.4 is no, please answer questions 1.6 to 1.21 and section B for further locations.
1.6	Is the server room windowless? ☒ yes ☐ no
1.7	If 1.6 yes: Please describe anti-intrusion and anti-burglar measures in respect to the windows ☐ barred ☐ alarmed ☐ lockable ☐ not at all ☐ Other: Please specify
1.8	Is the server room equipped with an alarm system? ☒ yes ☐ no
1.9	If 1.8 yes: Who is informed if the alarm system is triggered? Multiple answers possible! ☒ Security company ☒ Administrator ☒ IT manager ☐ Other: please specify
1.10	Is the server room equipped with CCTV (video surveillance)? ☐ yes, without image recording ☒ yes, with image recording ☐ no

1.11	If 1.10 yes, with image recording: For how long is the video footage stored? 30 days
1.12	How many people have access to the server room and which functions do they have? Number of persons: ca. 10 persons Function within the company: please specify the role of the relevant persons
1.13	Is the server room equipped with an electronic locking system? ☒ yes ☐ no, there is a mechanical lock
1.14	If 1.13 yes: Which access technology is used? Multiple answers possible! ☒ RFID ☒ PIN ☐ Biometrics ☐ Other: please specify
1.15	If 1.13 yes: Are access rights assigned individually? ☒ yes ☐ no
1.16	If 1.13 yes: Are access-attempts to the server room logged within the system? ☒ yes, successful as well as unsuccessful attempts ☐ yes, but only successful accesses ☐ yes, but only unsuccessful attempts ☐ no, the lock will only be released or not.
1.17	If 1.16 is yes: For how long is the access data stored before deletion? 100 days
1.18	If 1.13 no: How many keys to the server room exist, where are they kept and who distributes them? Number of keys: Number of keys Location: Specify location Person/Function responsible for distributing keys: please specify
1.19	What is the access door to the server room made of? ☒ Steel / Metal ☐ Other material
1.20	Is the server room being used for other purposes as well besides its actual function? ☐ yes ☒ no
1.21	If 1.20 yes: What else is kept in the server room? ☐ Telephone system ☐ Storage of office supplies ☐ Storage of files ☐ Archive ☐ Storage of IT equipment ☐ Other: please specify
2.	Access control measures to the office rooms
2.1	Location(s) of the client workstations, from which personal data are accessed: Bremen
2.2	Is there a porter service / a constantly occupied lobby in the building / office space? ☒ yes ☐ no
2.3	Do you have a visitor’s book? ☒ yes ☐ no

2.4	Is the building or the office space protected by a burglar alarm system? ☒ yes ☐ no
2.5	If 2.4 yes: Who is informed if the alarm system is triggered? Multiple answers possible! ☒ Security company ☒ Administrator ☒ IT manager ☐ Other: please specify
2.6	Is a CCTV system (video surveillance) installed at the office building or its entrances? ☒ yes, without image recording ☐ yes, with image recording ☐ no
2.7	If 2.6 yes, with image recording: For how long is the video footage stored? please insert a value in days days
2.8	Is the building / office space equipped with an electronic locking system? ☒ yes, building and office rooms are electronically locked ☐ yes, but only the building, not the entrance to the office space or to the floor on which the offices are located ☐ yes, but only the entrance to the offices / the floor on which the offices are located, not the entire building ☐ no
2.9	If 2.8 yes: Which access technology is used? Multiple answers possible! ☒ RFID ☐ PIN ☐ Biometrics ☐ Other: please specify
2.10	If 2.8 yes: Are access rights assigned individually? ☒ yes ☐ no
2.11	If 2.8 yes: Are access-attempts to the server room logged within the system? ☒ yes, successful as well as unsuccessful attempts ☐ yes, but only successful accesses ☐ yes, but only unsuccessful attempts ☐ no, the lock will only be released or not.
2.12	If 2.11 yes: For how long will access data be stored before deletion? 730 days
2.13	If 2.11 yes: Are the access logs reviewed regularly? ☐ yes ☒ no, but a review would be possible if required
2.14	Is the building/office space equipped with a mechanical lock? ☒ yes ☐ no
2.15	If 2.14 yes: Is the key distribution documented, and who distributes the keys? ☒ yes ☐ no Responsible person: Please specify
2.16	Is there an official access policy for visitors to the premises? ☐ no ☒ yes, visitors will be received at the entrance / reception by the contact person and must be accompanied at all times
3	Access control measures to the system

3.1	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? ☒ Defined distribution process ☐ No defined distribution process, on demand ☐ Other: please specify
3.2	Is assigning or changing the access information recorded? ☒ yes ☐ no
3.3	Do employees log in via an individual authorization in the central directory service? ☒ yes ☐ no
3.4	Are binding password parameters in operation? ☒ yes ☐ no
3.5	Password character length: min. 8 Do the password require to include special characters? ☒ yes ☐ no Expiration period in days: max. 100 days
3.6	Does the IT system enforce compliance with the above-mentioned password criteria? ☒ yes ☐ no
3.7	Does the screen lock automatically after a defined length of inactivity? If yes, after how many minutes? 3 minutes
3.8	Which measures are taken when a password is lost, forgotten or compromised? ☒ Admin issues a new initial password ☐ None
3.9	Is there a limited number of unsuccessful log in attempts? ☒ yes, 5 attempts ☐ no
3.10	If 3.8 yes, How long will access be denied, when the maximum number of unsuccessful attempts has been reached? ☐ Access will be revoked until it is manually reinstated ☒ Access will remain locked for 15 minutes
3.11	How is authorized remote access authenticated? ☐ Token ☒ VPN-Certificate ☒ Password
3.12	Is there a limited number of unsuccessful remote log in attempts? ☒ yes, 5 attempts ☐ no
3.13	How long will access be denied, once the maximum number of unsuccessful attempts has been reached? ☐ Access will be revoked until it is manually reinstated ☒ Access will remain locked for 15 minutes

3.14	Is the remote access disconnected after a defined period of inactivity? ☒ yes, after 30 minutes ☐ no
3.15	Are the systems that process personal data secured by a firewall? ☒ yes ☐ no
3.16	If 3.15 yes: Is the firewall updated regularly? ☒ yes ☐ no
3.17	If 3.15 yes: Who administers the firewall? ☒ Own IT department ☐ External service provider
3.18	If an external service provider is in use: Can the firewall be accessed from outside without supervision by the IT department? ☐ yes ☒ no, access is only possible following the four-eyes principle with an employee of IT.
4	Measures for the assurance of paper documents, mobile data carriers and mobile devices
4.1	How are documents containing personal information (e.g. printouts / files / correspondence) disposed of? ☐ wastepaper / trash bin ☒ shredders (employees are instructed to use them) ☒ Data security bins which are collected by a certified service provider for document destruction. ☐ Other: please specify
4.2	How are data carriers containing personal information (e.g. USB sticks, hard disks) disposed of? ☒ physical destruction by the internal IT department ☒ physical destruction by an external service provider ☒ Deletion of data by overwriting number of overwrites: ☐ Other: please specify
4.3	Is the use of mobile data carriers generally permitted (e.g. USB sticks)? ☒ yes ☐ no
4.4	May employees use their own personal data carriers (e.g. personal USB sticks)? ☐ in general, yes ☐ yes, but only after clearance by the IT department ☒ no, all required storage media are provided by the company
4.5	Is personal data on mobile devices encrypted? ☒ Encrypted hard drive ☐ Encryption of individual processes ☐ No measures

4.6	Do employees process personal data on their own personal devices (bring your own device)? ☐ yes ☒ no
5	Measures for secure data transfer
5.1	Are all data transfer processes completely encrypted? ☐ no at all ☐ no, data transfer only per MPLS ☐ only individually ☐ an encrypted file as e-mail attachment ☐ via PGP/SMIME ☐ via an encrypted data carrier ☒ via VPN ☒ via https/TLS ☒ via SFTP ☐ Other: please specify
5.2	Who is responsible for the administration of keys / certificates? ☐ Administrator ☒ Internal IT ☐ External service provider
5.3	Are all data transfers logged? ☒ yes ☐ no
5.4	If 5.2 yes: For how long is the log data retained? Depending on the legal storage obligation
5.5	If 5.2 yes: Are log files reviewed regularly? ☐ yes ☒ no, but a review would be possible if required

B. Measures for the assurance of availability

1.	Server rooms
1.1	Is the door to the server room fire-proof / fire-resistant? ☒ yes ☐ no
1.2	Is the server room equipped with smoke detectors? ☒ yes ☐ no
1.3	Is the server room connected to a fire alarm control panel? ☒ yes ☐ no
1.4	Is the server room equipped with extinguishing systems? Multiple answers possible! ☒ yes, CO2 extinguishers ☐ yes, Halon / Argon extinguishing system ☐ others: please specify

1.5	Please describe the material of the external walls of the server rooms. ☐ solid wall (e.g. concrete) ☐ lightweight construction ☒ Fireproof wall (e.g. F90)
1.6	Is the server room air-conditioned? ☒ yes ☐ no
1.7	Does the server room have an uninterruptible power supply (UPS)? ☒ yes ☐ no
1.8	Is the power supply to the server room also backed-up by a diesel-powered generator? ☒ yes ☐ no
1.9	Are the functionalities in 1.2, 1.3, 1.4, 1.6, 1.7 and 1.8, where present, tested regularly? ☒ yes ☐ no
2	Backup- and emergency concepts, virus protection
2.1	Is a backup concept in place? ☒ yes ☐ no
2.2	Is the backup-recovery functionality tested regularly? ☒ yes ☐ no
2.3	How often are backups made from systems containing personal data? ☐ Real time ☒ Daily ☐ One to three times a week ☐ Other: Please specify
2.4	Which storage medium is used for backups? ☒ Second redundant server ☐ Backup Tapes ☐ Hard drives ☐ Other: please specify
2.5	Where are the backups stored? ☒ Second redundant server in a separate location ☐ fireproof document and data carrier safe ☐ standard safe ☐ bank safe deposit box ☐ lockable desk drawer / filing cabinet ☐ in the server room ☐ private residence ☐ Other: please insert storage location
2.6	Regarding 2.5: If backups are transported: how are transports carried out? ☐ Transport by an IT employee / Management / Secretary ☐ Collection by a third party (i.e. bank employees / security company) ☒ Other: No transport of Backups
2.7	Are the backups encrypted? ☐ yes ☒ no
2.8	Is the backup storage location in a separate fire compartment or building from the primary server? ☒ yes ☐ no
2.9	Do you have a policy / process description for software or patch-management?

	☒ yes ☐ no ☐ Process is in place, but is not documented
2.10	If 2.9 yes, who is responsible for the software or patch management? ☐ Administrators ☒ Internal IT ☐ External service provider
2.11	Is an emergency plan in place (emergency measures in the event of an emergency, hardware defects, fire, data loss, etc.)? ☒ yes ☐ no
2.12	Are the IT systems technically protected from data loss / unauthorized data access? Yes, by up-to-date ☒ Virus protection ☒ Anti-Spyware ☒ Spam filter
2.13	If 2.12 yes, who is responsible for maintaining virus protection, spyware and spam filter up-to-date? ☐ Administrators ☒ Internal IT ☐ External service provider
3	Network connection
3.1	Does the company have a redundant internet connection? ☒ yes ☐ no
3.2	Are the company's various sites connected by a redundant connection? ☒ yes ☐ no
3.3	Who is responsible for the company's network connection? ☒ Internal IT ☐ External service provider

C. Pseudonymization/Encryption, Art. 32 (1) lit. a GDPR

1.	Pseudonymization
1.1	Is personal data pseudonymized? ☐ yes ☒ no
	If 1.1 no: please go to C2.
1.2	Is the pseudonymization based on algorithms? ☐ yes ☐ no
1.3	If 1.1 yes: Please provide further details regarding the algorithms in use. Please specify.
1.4	Are the keys to re-identify the data subject stored separately and in a separated system? ☐ yes ☐ no
1.5	How can the pseudonymization be undone if necessary? Multiple answers possible! ☐ based on a defined procedure ☐ multi-eye principle ☐ Direct access to non-pseudonymized raw data

	☐ On instruction of the supervisor ☐ Other: please specify
2.	Encryption
2.1	Is processed personal data encrypted beyond the measures described above? ☐ yes ☒ no
	If 2.1 no: please go to D1.
2.2	What types of encryption are used? Multiple answers possible! ☐ End-to-end-encryption ☐ transport encryption ☐ Data-at-rest-encryption ☐ Other: please specify
2.3	Which cryptographic algorithms are used for encryption or for encryption-like measures (e.g. hashing of passwords)? ☐ AES ☐ SHA-256 ☐ RSA-2048 or higher ☐ other: please specify
2.4	Who has access to the encrypted data? Employees of the departments: please specify A total number of ... employees have access to the encrypted data.

D. Further Controls acc. to Art. 32 (1) lit. b, c, d GDPR

1.	Resilience
	Measures exist to ensure the ability to ensure the long-term resilience of systems and services with regard to the processing ☒ no ☐ yes please specify the measures
2	Ability to restore the availability and access to personal data
	Are emergency and recovery plans and measures in place that go beyond B.2.11 to ensure the ability to quickly restore the availability of and access to personal data in the event of a physical or technical incident? ☒ no ☐ yes please specify the measures
3	Process for testing and evaluating the effectiveness of technical and organizational measures
3.1	Is there a procedure for regular review, assessment and evaluation of the effectiveness of technical and organizational measures to ensure security of processing?

	☐ no ☐ yes ISO27001 - Audits
3.2	If 3.1 yes: How often / at what intervals are these measures tested? Once per year
3.3	If 3.1 yes: Are the test results documented? ☒ yes ☐ no
3.4	Has the company been certified with regard to technical-organizational measures? And if so, which? ☒ yes, ISO27001 ☐ no