univention
be open.

Data Processing Agreement

between

– hereinafter referred to as ”Controller” –

and

Univention GmbH

Mary-Somerville-Straße 1

28359 Bremen

– hereinafter referred to as the ”Processor” –

– and collectively referred to as ”the Parties” –

is hereby agreed as follows:

§ 1 Subject matter and Term

The Processor shall carry out the data processing listed in Annex 1. It shall describe the subject matter, nature, purpose and duration of the processing as well as the categories of data processed and data subjects.

§ 2 Instructions by the Controller

1 The Processor shall process personal data only for the purposes listed in Annex 1 or on documented instructions from the Controller, unless the Processor is required to process certain personal data by law of the Union or a Member State to which the Processor is subject. In such a case, the Processor shall notify the Controller of those legal requirements prior to the processing, unless the law in question prohibits such notification on grounds of substantial public interest.

2 The Processor shall immediately inform the Controller if, in its opinion, an instruction of the Controller infringes the Union or a Member State data protection law.

3 Processing of the personal data provided by the Controller for other purposes than listed in

Annex 1, in particular for its own purpose, is not permitted.

§ 3 Technical and organisational measures

1 The Processor shall undertake to implement the technical and organisational measures specified in Annex 3 to ensure the security of personal data. The measures shall ensure a level of protection appropriate to the risk involved in processing the data in scope of this Agreement. In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context, purposes of the processing and categories of data (in particular pursuant to Article 9(1) or Article 10 of the GDPR), as well as the different probabilities of occurrence and the severity of the risk for the data subjects.

2 The technical and organisational measures listed in Annex 3 are subject to technical progress and further development. They shall be adapted by the processor if the agreed level of security can no longer be guaranteed. The adaptation may only be carried out if they at least provide the same level of protection achieved when previous measures were in force. Unless otherwise stipulated, the Processor shall notify the Controller of the adjustments made willingly and without undue delay.

§ 4 Obligations of the processor

1 The Processor confirms that it is aware of the relevant data protection regulations. The Processor shall organise the internal operating procedures within its area of responsibility in such a way that it meets the special requirements of an effective data protection management program.

2 The Processor shall grant access to the personal data undergoing processing to only to those employees familiar with the Data Protection Law in force and to the extent strictly necessary for implementing, managing and monitoring of the Agreement. The Processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3 To the extent required by law, the Processor shall appoint a data protection officer and provide his/her contact details in Annex 1. The Processor shall inform without delay and unrequested about any change of the Data Protection Officer.

4 The Processor shall carry out the processing in the territory of the Federal Republic of Germany, in a Member State of the European Union or within the European Economic Area. Any transfer of data to a third country by the Processor shall be done only on the basis of documented instructions from the Controller and shall take place if the specific legal requirements of the

GDPR are met.

§ 5 Assistance to the Controller

1 The processor shall promptly notify the controller of any request it has received from the data subject. The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing.

2 In addition to the processor's obligation to assist the controller pursuant to Clause 5(1), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

2.a the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment');

2.b the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

3 The Processor shall provide assistance in reviewing data breaches and implementing any notification obligations, as well as in complying with the obligation to ensure that personal data is accurate and up to date.

4 Furthermore, the Processor shall assist with appropriate technical and organizational measures to enable the Controller to fulfill its existing obligations towards the data subject.

§ 6 Use of sub-processors

1 The Processor may only engage sub-processors that are not already specified in Annex 2 if the Controller has given its prior written authorisation. The Processor shall submit the request for specific authorisation at least three weeks prior to the engagement of the sub-processor in question, together with the information necessary to enable the Controller to decide on the authorisation. The use of the sub-processors listed in Annex 2 shall be considered authorised, provided that the prerequisites set out in Section 6(2) of this Agreement are implemented.

2 Where the Processor engages a sub-processor for carrying out specific processing activities (on behalf of the Controller), it shall do so by way of a written contract, which may also be concluded in an electronic format, which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with the clauses

in this Agreement. At the Controller's request, the Processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the Controller. The Processor shall remain fully responsible to the Controller for the performance of the sub-processor's obligations in accordance with its contract with the Processor. The Processor shall notify the Controller of any failure by the sub-processor to fulfil its contractual obligations without undue delay.

3 The Processor shall ensure compliance with the provisions of Articles 44 to 50 of the GDPR in the event of a subcontracting involving a transfer of personal data within the meaning of Chapter V of the GDPR by providing, where necessary, appropriate safeguards in accordance with Article 46 of the GDPR.

4 Where the Processor engages a sub-processor in processing activities which involves a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the Processor and the sub-processor shall ensure compliance with Chapter V of GDPR by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) GDPR, provided the conditions for the use of those standard contractual clauses are met.

5 In the case of Section 6(4), the Processor shall carry out the assessment in accordance with Articles 14 and 15 of the Standard Contractual Clauses and make it available to the Controller upon request. If the Processor or the Controller come to the conclusion that further measures need to implemented to ensure an adequate level of protection, these measures shall be implemented by the Processor or the sub-processor respectively. The sub-processor may only be involved in the data processing once an adequate level of protection has been ensured.

§ 7 Documentation and compliance

1 The Processor shall provide the Controller with all information necessary to demonstrate compliance with the obligations set out in this Agreement and adapted directly from the GDPR. At the Controller's request, the Processor shall also allow and contribute to audits of the processing activities covered by this Agreement, at reasonable intervals or if there are indications of non-compliance of any required regulations. In deciding on a review or an audit, the Controller may take into account relevant certifications within the meaning of Article 28(5) GDPR held by the Processor.

2 The Controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the Processor and shall, where appropriate, be carried out with reasonable notice and in a manner that complies with the Processor's business and confidentiality obligations and, where possible, without disrupting operations.

3 The Parties shall make the information referred to in this Agreement, including the results of any audits, available to the competent supervisory authority/ies on request.

§ 8 Infringements to be notified

1 The Processor shall inform the Controller without undue delay of any disruptions to operations that entail risks for the Controller's data, as well as when data protection breaches in connection with the Controller's data become known. The same shall apply if the Processor establishes that the security measures taken by the Processor do not meet the legal requirements.

2 The Processor is aware that the Controller is under an obligation to comprehensively document all breaches of personal data protection and, if necessary, to report them to the supervisory authority/ies or the data subject. The Processor shall notify the Controller without undue delay after the Processor having become aware of the breach. Such notification shall contain, at least:

- Description of the nature of the breach, including, where possible, the categories and approximate number of individuals and data sets affected,
- Name and contact details of contact persons for further information,
- a description of the likely consequences of the injury, and
- a description of the measures taken or proposed to correct the breach or mitigate the resulting adverse effects.

§ 9 Termination

1 Following termination of the Agreement, the Processor shall delete or return all personal data processed on the behalf of the Controller unless the Union or a Member State law requires storage of the personal data. This shall also apply to any existing copies in accordance with the technical and organizational measures taken. The Processor shall notify the Controller of the deletion and return of the data in writing.

2 The Controller may terminate the contractual relationship without notice if the Processor commits a serious breach of the provisions of this Agreement or of data protection regulations and the Controller cannot reasonably be expected to continue the contractual relationship until the conclusion of the notice period or until the agreed termination of the Agreement.

3 The Processor may terminate the contractual relationship without notice if the Controller insists on the fulfilment of its instructions even though such instructions violate applicable legal requirements or this Agreement and the Processor has notified the Controller thereof.

§ 10 Accession to the Agreement

Any entity that is not a Party to this Agreement may, with the agreement of all the Parties, accede to this Agreement at any time as a controller or a processor by means of a declaration of accession. In addition to the declaration of accession, Annexes 1 to 3 shall be completed where necessary. From the date of accession, the acceding entity shall be treated as a Party to this Agreement and have the rights and obligations of a controller or a processor, in accordance with its designation.

§ 11 Final provisions

1 If the property of the Controller which is held by Processor is at risk by actions of third parties (for example by attachment or seizure), by insolvency proceedings or by other events, the Processor shall notify the Controller immediately. A right of retention is excluded with regard to data carriers and data files of the Controller.

2 The grounds for the Agreement, amendments to the Agreement and ancillary agreements must be in writing, which may also be in an electronic format.

3 In the event of any conflict between these contractual clauses and the provisions of related agreements existing between the parties or subsequently entered into or concluded, these clauses shall prevail.

4 Should any provision of this Agreement become invalid, that shall not affect the validity rest of the Agreement.

5 This contract is valid without signature by the contracting parties.

Annex 1

Description of processing

Subject matter of the processing	Support and remote maintenance services for the fulfilment of the concluded service contract.
Nature and purpose of the processing	Maintenance and support of the software solution provided by the processor. (Cooperation partner)
Categories of personal data processed	Depending on the order and the concluded service contract concluded, the following personal data may be affected: master data, contact data, communication data, functional data, telemetry data, diagnostic data, protocol data
Categories of data subjects whose personal data is processed	Depending on the support or remote maintenance order and theservice contract concluded, the following persons may be persons may be affected: Employees, customers, Software users
Duration of the processing	Corresponds to the duration of the Subscription Agreement

Controller's data protection officer	
Processor's data protection officer	Oliver Stutz datenschutz nord GmbH Konsul- Smidt-Straße 88 28217 Bremen

Annex 2

List of sub-processors used, including processing sites

Sub-processor	Processing site	Description of the processing
Bremen Briteline GmbH Wiener Str. 5 28359 Bremen	Wiener Str. 5 28359 Bremen	Provision of computing power and server capacity, data storage
IONOS SE Elgendorfer Str. 57 56410 Montabaur	Elgendorfer Str. 57 56410 Montabaur	Provision of computing power and server capacity, data storage
PlusServer GmbH Venloer Straße 47 50672 Köln	Venloer Straße 47 50672 Köln	Provision of computing power and server capacity, data storage

univention
be open.

Annex 3

Technical and organisational measures according to Article 32 GDPR

A – Measures to Ensure Confidentiality and Integrity

A1. Access Control for Server Rooms

No.	Question	Answer
1.0	Is personal data of the Controller stored on servers operated by you or any service providers?	☑ yes ☐ no
1.1	Location of the server room / data center (DC).	**Bremen Briteline GmbH, Wiener Straße 5, 28359 Bremen**
1.2	Is the personal data distributed across more than one server location or data center?	☑ yes ☐ no
1.3	(If 1.2 yes:) Further server locations:	IONOS SE, Elgendorfer Str. 57, 56410 Montabaur; PlusServer GmbH, Venloer Straße 47, 50672 Köln
1.4	Do the following details regarding access control measures apply to all data centers and server locations currently in use?	☐ yes ☑no (Details refer primarily to the Briteline DC in Bremen; IONOS and PlusServer operate their own certified security concepts)
1.5	(If 1.4 no:) Please answer questions 1.6 to 1.21 for further DC locations.	Note acknowledged. IONOS is ISO 27001 certified. PlusServer is certified according to ISO 27001, BSI C5, IDW PH 9.860.1

		and ISAE 3402.
1.6	Does the data center have windows?	No (Briteline data center, TSI Level 2 certified)
1.7	(If 1.6 yes:) How are the windows protected against intrusion?	N/A
1.8	Is the data center secured with an intrusion detection system (IDS)?	Yes (Operation according to TSI Level 2 IT security concept)
1.9	(If 1.8 yes:) Who is notified if the IDS is triggered?	No specific information provided
1.10	Is the data center under video surveillance?	☑ yes (Briteline monitors the premises via a video surveillance system) no
1.11	(If yes, with image recording:) How long is the video footage stored?	2-4 weeks
1.12	How many people have access to the server room and what are their roles?	**Only authorized employees of Univention GmbH**; access exclusively in combination with RFID token and PIN. Exact number: no specific information provided.
1.13	Is the data center equipped with an electronic locking system?	☑ yes ☐ no, with mechanical lock
1.14	(If 1.13 yes:) Which access technology is used?	☑ RFID ☑ PIN ☐ Biometrics

1.15	(If 1.13 yes:) Are access rights assigned on a personalized basis?	☑ yes ☐ no (Access only for explicitly authorized employees)
1.16	(If 1.13 yes:) Are access events logged in the access system?	No specific information provided
1.17	(If 1.16 yes:) Approximately how long is the access data stored?	No specific information provided
1.18	(If 1.13 no:) Number of keys, storage location, point of issue?	N/A (electronic system)
1.19	What material is the access door to the data center made of?	No specific information provided (Briteline DC, TSI Level 2)
1.20	Is the data center used for other purposes in addition to its primary function?	No specific information provided
1.21	(If 1.20 yes:) What else is stored there?	N/A

A2. Access Control for Offices

No.	Question	Answer
2.1	Location of the client workstations from which personal data is accessed:	**Mary-Somerville-Straße 1, 28359 Bremen; Mariannenstr. 9-10, 10999 Berlin; Egelstr. 4, 04103 Leipzig**
2.2	Is there a porter service or a constantly staffed reception area?	No specific information provided
2.3	Is a visitor log maintained?	No specific information provided

2.4	Is the building or are the office rooms secured with an intrusion detection system (IDS)?	No specific information provided
2.5	(If 2.4 yes:) Who is notified if the IDS is triggered?	N/A
2.6	Is the office building or its access points under video surveillance?	No specific information provided
2.7	(If 2.6 yes, with image recording:) Retention period?	N/A
2.8	Is the building or are the office rooms equipped with an electronic locking system?	☑ no – At all locations, access is provided via a mechanical locking system.
2.9	(If 2.8 yes:) Access technology?	N/A
2.10	(If 2.8 yes:) Are access rights assigned on a personalized basis?	N/A
2.11	(If 2.8 yes:) Are access events logged?	N/A
2.12	(If 2.11 yes:) Retention period for log data?	N/A
2.13	(If 2.11 yes:) Are logs evaluated regularly?	N/A
2.14	Is there a mechanical lock for the building or office rooms?	☑ yes ☐ no
2.15	(If 2.14 yes:) Is key issuance logged, who issues them?	☑ yes – Key issuance is logged. The loss of a key must be reported. A defined process for employees leaving the company

		ensures the return of the keys.
2.16	Are there official access regulations for third parties?	No specific information provided; all doors and windows are checked for proper closure at the end of business hours.

A3. Physical and Logical Access Control Measures

No.	Question	Answer
3.1	Is there a process for assigning user IDs and access permissions?	☑ **Defined approval process** – There is a defined process for suspending accounts and revoking permissions granted to departing employees.
3.2	Are the assignment or changes of access permissions logged?	No specific information provided
3.3	Do employees authenticate themselves using an individual ID to the central directory service?	☑ yes – A valid user account in the internal identity management system is required. The user account must be authorized for the respective system or application.
3.4	Are there binding password parameters within the company?	☑ yes – Univention password policy according to BSI recommendations
3.5	Password parameters:	**Character length:** Minimum password length (exact number not specified) **Special characters:** ☑ yes

		(various character types required, common dictionary entries prohibited) **Validity period:** No specific information provided
3.6	Does the IT system force the user to comply with the password specifications?	☑️ yes (implicitly, as the password policy is technically enforced)
3.7	Is the screen locked upon inactivity?	☑️ yes – All employees are instructed to lock the screen when leaving their workstation. Additionally, the screen is locked automatically upon inactivity. Exact duration: no specific information provided.
3.8	Measures in case of loss/forgetting/compromise of a password?	☑️ **User must then change the initial password.** (implicitly via the identity management system)
3.9	Is there a limit on unsuccessful login attempts?	No specific information provided
3.10	(If 3.9 yes:) How long do accounts remain locked?	N/A
3.11	How is authentication performed for remote access?	☑️ **VPN certificate** (personal SSL certificate) ☑️ **Password** – VPN connections require a personal SSL certificate and an activated user account. Employees are activated only after receiving specific instruction.
3.12	Limit on unsuccessful login	No specific information

	attempts for remote access?	provided
3.13	(If 3.12 yes:) Lockout duration?	N/A
3.14	Is remote access automatically disconnected after a certain period of inactivity?	☑ **yes** – After a limited period of "inactivity" by the Processor's personnel, the connection is forcibly disconnected. Exact number of minutes: no specific information provided.
3.15	Are the systems secured by a firewall?	Yes
3.16	(If 3.15 yes:) Is the firewall updated regularly?	Yes
3.17	(If 3.15 yes:) Who administers the firewall?	By Univention IT
3.18	(If external service provider:) Is access without supervision possible?	No specific information provided

A3-E. Supplementary Internal Policies and Agreements: Secure Remote Work

A3-E.1 Scope and Purpose

All employees of Univention GmbH who access internal IT systems, applications, or personal data from outside the office locations (Bremen, Berlin, Leipzig) – whether working from home, while traveling, or at other external work locations – are subject to the following binding regulations. The objective is to ensure a level of security equivalent to that of the office workplace and to reliably prevent unauthorized access to personal or confidential data.

A3-E.2 Mandatory VPN Use as a Central Security Element

Regulation	Content
Principle of Exclusivity	Any remote access to internal systems, specialized applications and file shares must be conducted **exclusively via the corporate VPN without exception**. Direct connections via the public internet are organizationally prohibited.
Technical Enforcement	The VPN is configured for **split-tunneling**. Accordingly, only traffic to internal company resources is routed through the encrypted VPN tunnel, while all other traffic is routed directly via the end device's internet connection. Compliance with the Principle of Exclusivity is ensured through technical measures. Internal systems are configured such that they are accessible exclusively via the VPN tunnel; direct access from the public network is technically blocked. The VPN server configuration is centrally managed and cannot be modified by end users.
Certificate-based Authentication	VPN connections require the use of a **personal certificate issued by the internal company PKI** as well as a valid user account with a password.

A3-E.3 Requirements for Remote Workstations and End Devices

Requirement	Regulation
Exclusive Use of Company-Owned End Devices	Only end devices provided and configured by the IT department of Univention GmbH may be used to access internal systems and personal data. The use of private devices (Bring Your Own Device - BYOD) for business activities involving

	access to internal systems is prohibited.
Full Disk Encryption	All business mobile end devices (notebooks, tablets) have fully encrypted drives. Before a new device is put into operation, the IT department verifies that encryption has been correctly configured.
Up-to-date Security Updates	Remote end devices must always be kept up to date with the latest operating system and security updates. Systems that do not comply with the current patch level are excluded from VPN access via technical controls (Network Access Control / Endpoint Compliance Check).

A3-E.4 Handling of Personal Data during Remote Work

Regulation	**Content**
No Local Storage of Personal Data	Personal data of the Controller must not be stored permanently on local drives of the remote end device. Processing takes place exclusively on the central server systems accessible via VPN.
Encrypted Transmission	Any transmission of personal or confidential data shall take place exclusively via encrypted channels (VPN, HTTPS/TLS, SSH, SFTP, PGP/S/MIME). Unencrypted transmission via email or file transfer is prohibited.
No Use of Private Cloud Services	Storing or transferring business data via unauthorized cloud services (e.g., private Dropbox, Google Drive, or iCloud accounts) is strictly prohibited.
Duty to Report Security Incidents Immediately	Security incidents, loss of devices, or suspicion of

	unauthorized access must be reported to the IT department immediately so that accounts can be suspended, certificates revoked, and further measures can be initiated.

A3-E.5 Mandatory Instruction and Employee Commitment

Measure	Description
Initial Training	Prior to the initial activation of VPN remote access, every employee receives documented instruction on the applicable security policies for remote work. Access is granted only after written acknowledgment has been provided
Regular Follow-up Training	Training on data protection-relevant topics is conducted at regular intervals, explicitly addressing the specific requirements and risks associated with mobile working and data processing.
Declaration of Commitment	All employees are bound to confidentiality and the observance of data protection notices and policies (Declaration of Commitment). Violations may result in disciplinary action.
Access Management upon Termination	Upon the departure of an employee or in the event of organizational changes, VPN certificates are revoked immediately, user accounts are locked, and all granted remote access permissions are withdrawn. This process is defined and documented.

A3-E.6 Technical Control and Compliance Monitoring

Measure	Description
Logging of VPN Connections	The establishment and termination of VPN connections are logged (timestamp, user ID, connection duration). The log data is retained for a defined period and can be analyzed in the event of security incidents.
Regular Review of the Policy	The present regulation is reviewed, evaluated, and updated if necessary at least once a year as well as on an ad-hoc basis (e.g., following security incidents or technical changes). The results of the review are documented.

A4. Measures for Securing Paper Documents, Removable Storage Media, and Mobile End Devices

No.	Question	Answer
4.1	Disposal of paper documents no longer needed that contain personal data?	☑ **Shredders are available and their use is mandated** ☑ **Locked data bins** – Paper documents are destroyed using shredders and a data bin.
4.2	Disposal of data carriers no longer needed?	☑ **Deletion of data through multiple overwriting +** ☑ **Physical destruction** – Prior to disposal, data carriers are wiped through multiple random overwriting and are subsequently physically destroyed.

4.3	May removable storage media be used within the company?	No specific information provided
4.4	May employees use private storage media?	No specific information provided
4.5	Is personal data encrypted on mobile end devices?	☑ **Disk encryption** – On mobile end devices (e.g., notebooks), all data is stored on fully encrypted drives.
4.6	Do employees also process personal data on their own private devices (BYOD)?	☑ **no** – In accordance with the internal policy (cf. A3-E.3), the use of private devices for accessing internal systems and personal data is prohibited.

A5. Measures for Secure Data Transfer

No.	Question	Answer
5.1	Is the transfer of personal data consistently encrypted?	☑ **via PGP or S/MIME** (email encryption) ☑ **via VPN** (SSL certificate-based VPN, full-tunnel only) ☑ **via HTTPS/TL**S (upload service for files and diagnostic data) ☑ **via SFTP/SSH** (remote access by default via encrypted SSH protocol) **Others:** Symmetric (AES-128, AES-256) and asymmetric (RSA, Elliptic Curve) encryption methods

5.2	Who manages the keys or certificates?	☑ **in-house IT** (company PKI; personal SSL certificates are issued, managed, and revoked as necessary by the IT department)
5.3	Are the transfer processes logged?	☑ **yes** – The Controller logs the connections as required. The establishment and termination of VPN connections are logged server-side (cf. A3-E.6).
5.4	(If 5.3 yes:) How long is this log data retained?	No specific information provided (this is within the responsibility of the Controller or is defined internally)
5.5	(If 5.3 yes:) Are the logs evaluated regularly?	☑ **no, but evaluation would be possible if necessary** (on an ad-hoc basis, e.g., in the event of security incidents)

B – Measures to Ensure Availability

B1. Server Room

No.	Question	Answer
1.1	Does the server room have a fire-resistant or fire-retardant access door?	No specific information provided (Briteline DC, TSI Level 2 certified)
1.2	Is the server room equipped with smoke detectors?	☑ **yes** – The data center has various sensors for detecting hazards, such as fire or smoke development.

1.3	Is the server room connected to a fire alarm control panel?	No specific information provided (implicitly yes, via sensors and TSI Level 2 certification)
1.4	Is the server room equipped with fire suppression systems?	No specific information provided (TSI Level 2 requires corresponding equipment)
1.5	What are the external walls of the server room made of?	No specific information provided
1.6	Is the server room climate-controlled?	☑️ **yes** – The data center has a **redundant cooling system**.
1.7	Does the server room have an uninterruptible power supply (UPS)?	☑️ yes – The data center has a **redundant uninterruptible power supply**.
1.8	Is the power supply additionally backed up by a diesel generator?	No specific information provided
1.9	Are the functionalities tested regularly?	No specific information provided

B2. Backup, Disaster Recovery, and Anti-Malware

No.	Question	Answer
2.1	Is there a backup concept?	No specific information provided for general systems. **Note**: Personal data relating to customers are **deliberately not backed up**; such data are used temporarily for problem analysis only and are deleted without delay upon completion

		of the support activity.
2.2	Is the functionality of backup recovery tested regularly?	No specific information provided
2.3	At what interval are backups created?	No specific information provided
2.4	Type of backup media?	No specific information provided
2.5	Where are the backups stored?	No specific information provided
2.6	Transport of backups?	No specific information provided
2.7	Are the backups encrypted?	No specific information provided
2.8	Is the storage location of the backups in a separate fire compartment?	No specific information provided
2.9	Is there a documented process for software and patch management?	No specific information provided
2.10	(If 2.9 yes:) Who is responsible?	No specific information provided
2.11	Is there an emergency concept?	No specific information provided (implicitly yes, through DC redundancies and defined processes)
2.12	Technical protection against data loss / unauthorized access (antivirus, etc.)?	No specific information provided
2.13	(If 2.12 yes:) Who is responsible?	No specific information provided

B3. Internet Connection

No.	Question	Answer
3.1	Does the company have a redundant internet connection?	No specific information provided
3.2	Are the individual locations redundantly connected to each other?	No specific information provided
3.3	Who is responsible for the network connectivity?	No specific information provided

C – Pseudonymization / Encryption

C1. Use of Pseudonymization

No.	Question	Answer
1.1	Is processed personal data pseudonymized?	No specific information provided – The document primarily describes encryption measures. (If 1.1 no: Questions C1.2–C1.5 are not applicable)

C2. Use of Encryption

No.	Question	Answer
2.1	Is processed personal data encrypted?	☑️ **yes** – Connections for data transfers are always secured using encrypted methods. Full disk encryption for mobile end

		devices.
2.2	Which types of encryption are used?	☑ **Encryption in transit** (VPN/SSL, HTTPS/TLS, SSH, PGP, S/MIME) ☑ **Data-at-rest encryption** (fully encrypted drives on mobile end devices)
2.3	Which cryptographic algorithms are used?	☑ **AES** (AES-128, AES-256) ☑ **RSA-2048 or higher** (RSA) **Others**: Elliptic Curve Cryptography (ECC); PGP, S/MIME for email encryption
2.4	Who has access to the encrypted data?	Access to potentially personal data is granted based on the **need-to-know principle** and the internal permissions and roles concept. Access is provided only on an ad-hoc basis and as required in the case of assistance or support requests. Exact number and departments: no specific information provided.

D – Other Measures

D1. Resilience

Question	Answer
Are there measures to ensure the resilience of the systems?	☑ **yes** – The security of the encryption methods is reviewed at regular intervals. The data center (Briteline) has a redundant uninterruptible power supply (UPS) as well as redundant cooling. Use of several certified data centers (IONOS,

	PlusServer). Technical measures to ensure VPN availability guarantee the continuous possibility of secure remote access (cf. A3-E).

D2. Recoverability

Question	Answer
Are there emergency or recovery concepts for the rapid restoration of the availability of personal data?	No specific information provided beyond the infrastructure redundancies. (Note: No long-term storage measures/backups are carried out for client-related personal data in support. Data is deleted immediately after the support activity is completed.)

D3. Procedure for Review, Assessment, and Evaluation

No.	Question	Answer
3.1	Is there a procedure for the regular review, assessment, and evaluation of the effectiveness of the TOMs?	☑ **yes** – Univention GmbH has established a procedure for the regular review, assessment, and evaluation of the effectiveness of the technical and organizational measures implemented. The remote work policy (cf. A3-E.6) is included in this review procedure.
3.2	(If 3.1 yes:) At what intervals do the reviews take place?	At least **annually** as well as on an ad-hoc basis (e.g., after security incidents or significant technical changes)
3.3	(If 3.1 yes:) Are the results of the	No specific information

	reviews documented?	provided
3.4	Are there any certifications relating to the TOMs?	☑️ **yes**: - **Briteline GmbH (DC Bremen)**: TSI Level 2 - **IONOS SE**: ISO 27001 - **PlusServer GmbH**: ISO 27001, BSI C5 Cloud Security, IDW PH 9.860.1 Data Protection, ISAE 3402 - Univention GmbH itself: No specific information provided regarding its own certifications