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.

univention
be open.

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	Dr. Uwe Schläger datenschutz nord GmbH Konsul- Smidt-Straße 88 28217 Bremen

univention
be open.

Annex 2

List of sub-processors used, including processing sites

Sub-processor	Processing site	Description of the processing
IONOS SE Elgendorfer Str. 57 56410 Montabaur	Elgendorfer Str. 57 56410 Montabaur	Bereitstellung von Rechenleistung und Serverkapazitäten, Datenspeicherung
PlusServer GmbH Venloer Straße 47 50672 Köln	Venloer Straße 47 50672 Köln	Bereitstellung von Rechenleistung und Serverkapazitäten, Datenspeicherung

univention
be open.

Annex 3

Technical and organisational measures according to Article 32 GDPR

1 Overview

Both client and contractor must organize the internal organization in such a way that it meets the special requirements of data protection. The technical and organizational measures taken must ensure a level of protection appropriate to the severity of the risk or threat of damage to the party concerned. The measures must ensure the confidentiality, integrity, availability of the data and resilience of the systems. The fulfillment of these protection goals is particularly hindered by the risks of destruction, loss, alteration, unauthorized disclosure and unauthorized access. The measures described below include the specified technical and organizational measures of Univention GmbH for the provision of product support and support for the operation of an identity management platform.

2 Locations and physical access to locations

2.1 Office locations

The workstations used by the contractor to connect to the client's network are located in access protected rooms. On mobile devices, such as notebooks, all data is stored on fully encrypted storage devices.

Univention GmbH has th following office locations:

- Mary-Somerville-Straße 1, 28359 Bremen
- Mariannenstr. 9-10, 10999 Berlin
- Egelstr. 4, 04103 Leipzig

At all locations, access to the building and the respective premises is protected via mechanical locking systems. The issue of keys to employees is logged, the loss of a key is to be reported, a defined process on retirement of an employee ensures the return of issued keys. All doors and windows are checked for proper closure at close of business.

2.2 Data Center

The server operation for the data from the above-mentioned methods is carried out by Univention in a Bremen-based external data center, which is operated according to recognized principles of IT security and regulates access in accordance with the IT security concept of the data center operator,

Bremen Briteline GmbH, Wiener Straße 5, 28359 Bremen (TSI Level 2 certified). Access to our server systems is only possible for authorized employees using RFID-Tokens and a pin. The company Briteline provides purely infrastructural services here and has no access to the IT equipment of Univention. All physical access to the data center Is documented. The operator monitors the premises by means of a video surveillance system. The data center is equipped with a redundant, uninterruptible power supply, a redundant air conditioning system, as well as various sensors for the detection of sources of danger, such as fire or smoke.

Furthermore, external data centers are used to host parts of the infrastructure and applications. These are IONOS SE, Elgendorfer Str. 57, 56410 Montabaur and PlusServer GmbH, Venloer Straße 47, 50672 Cologne. IONOS is ISO 27001 certified and has no access to the hosted instances. Only authorized employees have access to the hardware and access it only for maintenance purposes. The company PlusServer is certified according to ISO 27001, BSI C5 Cloud Security, IDW PH 9.860.1 Data Protection and ISAE 3402.

3 Access to IT systems

Access to the IT systems of Univention GmbH is based on the internal security concept:

- A valid user account in the internal identity management system is necessary.
- The user account must be authorized for the respective system or application.
- Access is only possible via the wired office network or via a secure VPN connection (WLAN made available to employees also allows access via VPN only)
- VPN connections are based on the latest technical standards and require the possession of a personal SSL certificate and a user account that has been activated for establishing VPN connections.
- Employees are only unlocked to use VPN connections after a separate instruction.
- User accounts are protected by means of a password which, in terms of complexity and age, must comply with the Univention password policy. This includes a minimum password length and a minimum complexity (consisting of different character types and the prohibition of common dictionary entries). The password guideline corresponds to the common recommendations of the BSI.
- There is a defined process for blocking accounts and revoking granted authorizations of departing employees.

- Mobile devices with access to Univention internal IT systems use only encrypted data carriers.
- All employees are instructed to lock their screen when leaving the workplace. In addition, the screen is disabled when inactive.

Access to personal data in the context of the above-mentioned procedures is based on the internal rights and roles concept. The connections required for data transmissions are always secured wherever possible using established, encrypted procedures and secured using symmetrical (AES-128, AES-256) and asymmetrical (RSA, elliptic curves) encryption procedures. The security of these procedures is checked at regular intervals. A remote connection requires the prior technical approval of the client. The connection can be interrupted at any time by the client. After temporary "non-activity" of the contractor, the connection is forced to be disconnected. After completion of the remote maintenance measure, the connection is closed.

4 Handling of personal data

In principle, it is avoided to transfer personal data from the client's systems to the internal network of Univention. A transfer only takes place if it is necessary for analysis purposes, e.g. in technical support.

For the transmission of personal or sensitive data to us, we offer encrypted transmission channels, the sending of personal or otherwise sensitive data to customers is also encrypted. If, in individual cases, a customer does not use the encryption options or does not have the necessary infrastructure, all employees in contact with customers are instructed to inform the customer about the associated risks and to work towards future encrypted transmission.

The client logs the connections as required.

The type and extent of the transmission of this data is carried out in close consultation with the customer and should always take place via secure and encrypted channels; the customer and contractor agree jointly on the relevant procedures. These should meet recognised security standards, such as the use of symmetrical and asymmetrical encryption methods, and should be checked regularly.

For communication via e-mail, Univention offers the possibility to secure messages via asymmetric encryption mechanisms. Univention offers the PGP and S/MIME standards for sending and receiving e-mails.

For the transfer of larger files and diagnostic data, Univention offers an upload service that secures

the transmission paths via the HTTPS protocol.

Remote access to the client's systems is carried out by default via the encrypted SSH protocol and must be initiated by the client. The client can terminate the connection at any time.

The employees of Univention are bound to secrecy according to the company agreement. There are regular training on data protection relevant topics, which especially deal with the peculiarities and duties of the processing of customer data.

Paper shredders and a dedicated bin are used to destroy paper-based documents; data carriers to be disposed of are emptied before being disposed of by multiple, random overwriting and then physically destroyed.

In the above procedures, access to customers' potentially personal information or the provision of potentially personal information by customers is on an ad-hoc basis and only when needed in the case of customer support or support requests. The data is not processed, managed or stored for the customer, but only for problem analysis. The data are therefore basically copies or excerpts of data, the full data is always exclusively held by the customer. In addition, the data is only needed for a very limited period of time during the problem analysis. Therefore no action is taken that contribute to the long-term storage of this data on our site (e.g. no Backups of this data).

No subcontractors will be used to carry out the above procedures.

The Contractor has established a procedure for the regular review, evaluation and evaluation of the effectiveness of the technical and organizational measures taken to ensure the security of the processing.