IGEL UMSaaS Data Processing Agreement

between

the customer using IGEL SaaS Services in accordance
with the IGEL UMSaaS License Agreement

- hereinafter "Controller"-

and

IGEL Technology GmbH

Marie-Cunitz-Str. 7, 28199 Bremen, Germany

- hereinafter "Processor"-

1. Purpose and scope

(a) The purpose of this data processing agreement ("**Agreement**") is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

(b) The Controllers and Processors listed in **Annex I** have agreed to this Agreement inorder to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 as well as other applicable local regulations.

(c) This Agreement applies to the processing of personal data as specified in **Annex II**.

(d) **Annexes I** to **IV** are an integral part of the Agreement.

(e) This Agreement is without prejudice to obligations to which the Controller is subject by virtue of Regulation (EU) 2016/679.

(f) This Agreement does not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679.

2. Interpretation

(a) Where this Agreement uses the terms defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) This Agreement shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) This Agreement shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

3. Hierarchy

In the event of a contradiction between this Agreement and the provisions of related agreements between the Parties existing at the time when this Agreement are agreed or entered into thereafter, this Agreement shall prevail.

4. Docking clause

(a) 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 completing the Annexes and signing **Annex I**.

(b) Once the Annexes in (a) are completed and signed, 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 in **Annex I**.

(c) The acceding entity shall have no rights or obligations resulting from this Agreement from the period prior to becoming a Party.

5. Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the Controller, are specified in **Annex II**.

6. Obligations of the Parties

6.1. Instructions

(a) The Processor shall process personal data only on documented instructions from the Controller, unless required to do so by Union or Member State law to which the Processor is subject. In this case, the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the Controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The Processor shall immediately inform the Controller if, in the Processor's opinion, instructions given by the Controller infringe Regulation (EU) 2016/679 or the applicable Union or Member State data protection provisions.

(c) The instructions result in particular from the applicable agreement entered into between the parties, which governs the provision of products and services by the Processor. The Processor's applicable agreements and terms are available at: https://www.igel.com/terms-conditions/

6.2. Purpose limitation

The Processor shall process the personal data only for the specific purpose(s) of the processing, as set out in **Annex II**, unless it receives further instructions from the Controller.

6.3. Duration of the processing of personal data

Processing by the Processor shall only take place for the duration specified in **Annex II**.

6.4. Security of processing

(a) The Processor shall at least implement the technical and organizational measures specified in **Annex III** to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the data (personal data breach). 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 and purposes of processing and the risks involved for the data subjects.

(b) The Processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The Processor shall ensure that persons authorized to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) Insofar as it is legally required, the Processor shall appoint a Data Protection Officer, and its contact details are to be shared with the Controller for the purposes of making direct contact as established within **Annex I**.

6.5. Sensitive data

(a) If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("**Sensitive Data**"), the Processor shall apply specific restrictions and/or additional safeguards.

(b) Due to the nature of the services provided by the Processor, the Processor assumes that no Sensitive Data will be processed unless the Controller has explicitly informed the Processor in writing. If such a notification is made, both parties shall cooperate in good faith to develop an appropriate security concept for the processing of Sensitive Data. The Processor has the right to refuse to process Sensitive Data and to terminate the applicable agreement with the Controller should the Controller uphold the request to process sensitive data despite the Processor's refusal.

6.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with this Agreement.

(b) The Processor shall deal promptly and adequately with inquiries from the Controller about the processing of data in accordance with this Agreement.

(c) The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations that are set out in this Agreement and stem directly from Regulation (EU) 2016/679. At the Controller's reasonable request, the Processor shall also permit and contribute to audits of the processing activities covered by this Agreement, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the Controller may take into account relevant certifications held by the Processor.

(d) The parties will cooperate in good faith in order to mutually define the scope and time of the audit in advance. The audit will be performed by an independent auditor who is bound to confidentiality.

6.7. Use of sub-processors

(a) The Processor has the Controller's general authorisation for the engagement of sub-processors from an agreed list as set out in **Annex IV**. The Processor shall specifically inform in writing the Controller of any intended changes of that list through the addition or replacement of sub-processors at least one month in advance, thereby giving the Controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The Processor shall provide the Controller with the information necessary to enable the Controller to exercise the right to object. The Processor can suspend the data processing after receiving an objection until the parties have found a mutually acceptable solution. The Processor reserves the right to terminate any agreement with the Controller if the Processor is no longer able to perform the agreement due to the sub-processor's objection in accordance with this section.

(b) 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 contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the Processor in accordance with this Agreement. The Processor shall ensure that the sub-processor complies with the obligations to which the Processor is subject pursuant to this Agreement and to Regulation (EU) 2016/679.

(c) 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.

(d) The Processor shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the Processor has factually disappeared, ceased to exist in law or has become insolvent - the Controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

6.8. International transfers

(a) Any transfer of data to a third country or an international organization by the Processor shall be done only on the basis of documented instructions from the Controller, including, but not limited to those provided for the provision of the Processor's products and services ordered by the Controller, or in order to fulfil a specific requirement under Union or Member State law to which the Processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The Controller agrees that where the Processor engages a sub-processor in accordance with section 6.7. for carrying out specific processing activities (on behalf of the Controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the Processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

7. Assistance to the Controller

(a) The Processor shall promptly notify the Controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the Controller.

(b) 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. In fulfilling its obligations in accordance with (a) and (b), the Processor shall comply with the Controller's instructions

(c) In addition to the Processor's obligation to assist the Controller pursuant to section 7(b), 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:

(1) 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') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) 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 obligation to ensure that personal data is accurate and up to date, by informing the Controller without delay if the Processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679 and other applicable data protection regulation.

(d) The Parties shall set out in **Annex III** the appropriate technical and organisational measures by which the Processor is required to assist the Controller in the application of this Section as well as the scope and the extent of the assistance required.

8. Notification of personal data breach

In the event of a personal data breach, the Processor shall cooperate with and assist the Controller for the Controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 and other applicable data protection regulation, where applicable, taking into account the nature of processing and the information available to the Processor. In particular, the Processor shall notify the Controller without undue delay within the following 48 hours after the Processor having become aware of the breach affecting personal data of the Controller under this agreement. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

9. Non-compliance with the Agreement and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 or other applicable data protection regulation, in the event that the Processor is in breach of its obligations under this Agreement, the Controller may instruct the Processor to suspend the processing of personal data until the latter complies with this Agreement or the contract is terminated. The Processor shall promptly inform the Controller in case it is unable to comply with this Agreement, for whatever reason.

(b) The Controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with this Agreement if:

(1) the processing of personal data by the Processor has been suspended by the Controller pursuant to point (a) and if compliance with this Agreement is not restored within a reasonable time and in any event within one month following suspension;

(2) the Processor is in substantial or persistent breach of this Agreement or its obligations under Regulation (EU) 2016/679 or other applicable data protection regulation;

(3) the Processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to this Agreement or to Regulation (EU) 2016/679 or other applicable data protection regulation.

(c) The Processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under this Agreement where, after having informed the Controller that its instructions infringe applicable legal requirements in accordance with Clause 6.1 (b), the Controller insists on compliance with the instructions.

(d) Following termination of the contract, the Processor shall, at the choice of the Controller, delete all personal data processed on behalf of the Controller and, on reasonable request of the Controller, certify to the Controller that it has done so, or, return all the personal data to the Controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the Processor shall continue to ensure compliance with this Agreement.

10. Governing Law and Jurisdiction

(a) The present Agreement shall be governed by the law of the Federal Republic of Germany, excluding its conflict of law provisions.

(b) All disputes arising out of or in connection with this Agreement, including disputes on its conclusion, shall be resolved exclusively by the ordinary courts of Bremen, Germany.

(April 2025)

ANNEX I

LIST OF PARTIES

Controller(s):

1. Name: As set out in the Agreement.

2. Address: As set out in the Agreement.

3. Data Protection Officer or contact person for data protection: To be provided by the Controller on reasonable request.

Processor(s):

1. Name: As set out in the Agreement.

2. Address: As set out in the Agreement.

3. Data Protection Officer

datenschutz nord GmbH, Konsul-Smidt-Straße 88, 28217 Bremen, Germany

office@datenschutz-nord.de, +49 421 69 66 320

ANNEX II

DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed	Customer’s employees, Customer’s contractors
Categories of personal data processed	**1. Provision of UMSaaS** Any and all personal data of the Controller, provided by the Controller to IGEL through the use of the UMSaaS: • Customized device attributes for devices, e.g. User name, employee ID, • Directory names, e.g., office location • Profile names and descriptions, e.g. AVD_department, AVD_name The UMS includes the following device attributes by default. Depending on whether the device itself provides the data categories listed below, they will be processed in the UMS by IGEL: • System information • Device name • Site • Department • Cost Center • Asset ID • In-Service Date • Serial Number • Comment • Onboarded by (user email address) • Connected to • Directory Path • Unit ID • MAC Address • Last Boot Time • Network Name (at Boot Time) • Runtime since last Boot • Total Operating Time • Battery Level • CPU Speed (MHz) • CPU Type

	• Flash Size (MB) • Memory Size (MB) • Network Speed • Duplex Mode • Graphics Chipset 1 • Graphics Memory 1 (MB) • Graphics Chipset 2 • Graphics Memory 2 (MB) • Device Type • OS Type • BIOS Vendor • BIOS Version • BIOS Date • Boot Mode • Device Serial Number • Structure Tag • Last Firmware Update Time **2. Provision of support services:** By default, we collect the following personal information in the course of ticket processing: • Salutation (Mr / Mrs), • first name, surname, • user name, • telephone number, • e-mail address, • company address (relevant for certain legal company addresses) and, • log files (name, IP address) provided by the customer.
Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.	None
Nature of the processing	**1. UMSaaS:** Hosting of customers' personal data for the purposes of providing the UMSaaS service and

	using such data when necessary for the purpose of providing technical support **2. Support services:** Personal data will be processed for the purpose of providing technical support.
Purpose(s) for which the personal data is processed on behalf of the controller	**1. UMSaaS:** Provision and hosting of the UMSaaS to fulfil contractual obligations towards the customer in accordance with the Agreement. **2: Support services:** To verify whether the data subject is entitled to technical support including warranty (RMA) and license requests. In the event of a corresponding claim for the provision of technical support for data subjects with technical problems and response to product / implementation inquiries and for the purpose of providing such support
Frequency of the processing (continuous transfer or one-off)	Continuous for the duration of the (service) agreement with the customer.
Retention periods applied to personal data	1. UMSaaS: After the agreement is terminated or has ended the data will be deleted after a technical grace period. 2. Support Service: The retention and storage periods under applicable law shall apply.
For processing by (sub-) processors, also specify subject matter, nature and duration of the processing	See above under “Nature of processing” and “Purpose for which the personal data is processed on behalf of the controller” and Annex IV.

ANNEX III

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons, the Processor has implemented appropriate technical and organizational measures with regard to the processing of personal data in order to ensure an adequate level of security as indicated below.

The Processor is **ISO/IEC 27001** certified for the IT services relevant to the provision of UMSaaS and associated support services. The certification is available at www.igel.com or on request. The Processor and the Controller have agreed on the following technical and organizational measures, which are implemented by the Processor for the processing of customer personal data, and therefore apply to the processing of the personal data specified in **Annex II**:

Comprehensive remote maintenance support is provided across the following locations depending on time of day and language preference:

- IGEL Technology GmbH, Germany
- IGEL Technology Ltd, United Kingdom
- IGEL Technology Corporation, USA

If necessary, support services are performed by employees from home office. Furthermore, it is also possible that support services can be provided from different locations if the employees are on-call duty.

The basic systems for customer support are operated at different locations:

- A Customer Relationship Management System (CRM) is administered in Germany and hosted by Microsoft Inc.
- The Support Ticket System is administered by the Processor and hosted by ServiceNow Nederland B.V.
- Sharefile (a platform for the exchange of large amounts of data) is administered by the Augsburg site and hosted by Citrix Systems UK Ltd.

Please refer to **Annex IV** for further information regarding the sub-processors.

1. Access Control Measures (Physical and Logical) (Art. 32 (1) (b) GDPR)

Physical Access Control

- All server rooms are protected with electronic locking systems (e.g., PIN code or smart card) and mechanical locks.
- Access authorizations are assigned individually, reviewed regularly, and follow the need-to-know principle.
- All access attempts (successful and unsuccessful) are logged and monitored.
- The issuance and return of physical keys are recorded in a key register.
- Video surveillance is implemented at critical entry points and complies with signage and privacy rules.

Office Premises

- Office buildings are secured by intrusion detection systems and alarm systems.
- Visitors must register and be accompanied during their stay.
- Smartcard or token-based entry systems are implemented where applicable.
- Visitor access is logged via a digital registration system.

Logical Access Control/Authentication

- Authentication requires username and password.
- Multi-Factor Authentication (MFA) is used for all systems and remote access.
- Access is granted only after supervisor's approval and follows the principle of least privilege.
- Access is revoked immediately upon role change or employment termination.
- Session timeouts and workstation locking are enforced.
- Centralized identity and access management is implemented.
- Access rights are reviewed at least annually.
- Default and temporary passwords must be changed upon first login.
- Failed login attempts are limited to prevent brute-force attacks.

2. Encryption & Pseudonymization (Art. 32 (1) (a) GDPR)

- Data stored in the CRM and other critical databases is encrypted (e.g., Transparent Data Encryption).
- Data in transit is protected using TLS 1.2 or higher.
- Portable devices are encrypted using BitLocker or equivalent.
- Email communication with personal data uses encryption standards (S/MIME or PGP).
- Key management practices include secure storage, limited access, and rotation policies.
- Pseudonymization is applied to personal data sets where possible and appropriate.

3. Network Security (Art. 32 (1) (b) GDPR)

- Data Loss Prevention (DLP) is implemented via Microsoft 365 (Purview DLP).
- Information is classified into sensitivity levels (e.g., public, internal, confidential).
- DLP policies monitor and restrict unauthorized sharing or transfer of classified or personal data.
- Automated alerts and actions support internal data handling policies.
- Firewalls are implemented at all internet-facing boundaries.
- Network segmentation is used to separate critical systems.
- Intrusion Detection and Prevention Systems (IDS/IPS) are in place.
- VPN is mandatory for remote access with MFA.
- Wi-Fi networks are encrypted and segregated.

4. Media Protection (Art. 32 (1) (b) GDPR)

- Use of external storage media is restricted and governed by internal policy.
- Devices scheduled for reuse or disposal are securely wiped.
- Shredding and certified disposal is used for paper documents and obsolete storage media.

5. Data Backup (Art. 32 (1) (c) GDPR)

- Backups are performed regularly, encrypted, and stored in a physically separate location.
- Geo-redundant and fire-compartment separate storage locations are used.
- Periodic restore tests ensure backup integrity.
- UPS systems are in place.
- Backup and disaster recovery plans are documented and regularly tested.

6. Logging & Monitoring (Art. 32 (1) (b) GDPR)

- Access logs for systems and data are recorded and monitored.
- Logs include admin actions, authentication events, and access to sensitive data.
- SIEM (Security Information and Event Management) tools are used for anomaly detection.
- Retention periods for logs are defined according to compliance requirements.

7. Patch & Vulnerability Management

- Regular patch cycles are established for operating systems, applications, and firmware.
- Critical vulnerabilities are addressed within defined timelines.
- Vulnerability scanning is performed regularly.

8. Secure Software Development

- Secure development lifecycle (SDLC) is in place.
- Code reviews, static and dynamic testing, and dependency checks are conducted.
- Developers are trained in secure coding practices.

9. Information Security Management (Art. 32 (1) (d) GDPR)

- A formal Information Security Management System (ISMS) is established based on ISO/IEC 27001.
- Roles and responsibilities are clearly defined.
- Policies and procedures are reviewed annually.
- Security objectives are tracked and measured.

10. Responsibilities & Governance

- A Data Protection Officer (DPO) is appointed.
- Information Security Officers oversee technical controls.
- Responsibilities are documented and assigned using a RACI model.

11. Employee Training & Awareness

- All employees receive initial and ongoing data protection and security training.
- Awareness campaigns are conducted regularly.
- Specialized training is provided for developers and admins.

12. Supplier & Third-Party Management

- Where required under applicable law, Data Processing Agreements (DPAs) are in place for vendors which are processing personal data on IGEL’s behalf.
- Security due diligence is performed prior to onboarding vendors.
- Third-party risk assessments and reviews are conducted regularly.

13. Incident Management (Art. 33, 34 GDPR)

- A documented Incident Response Plan is maintained.
- Roles and escalation paths are defined.
- Security incidents are logged and investigated promptly.
- Breaches are reported to supervisory authorities within statutory notification periods, if applicable.
- Post-incident reviews identify root causes and improvements.

14. Risk Management (Art. 32 (1) (b) and (d) GDPR)

- Regular risk assessments are performed for systems and processing activities.
- Threat modeling and data protection impact assessments (DPIAs) are carried out where required.
- Risks are categorized and mitigated based on defined acceptance criteria.

15. Continuous Improvement (Art. 32 (1) (d) GDPR)

- Technical and organizational measures are reviewed annually or after significant incidents.
- Internal audits are conducted.

16. Confidentiality Commitments (Art. 32 (1) (b) GDPR)

- All employees and contractors sign confidentiality agreements.
- Data processors are contractually bound to confidentiality (Art. 28 (3)(b) GDPR).
- Confidentiality is enforced even after termination of employment or contract.

ANNEX IV

LIST OF SUB-PROCESSORS

Full legal name of contracted sub-processor	Address and possible, contact person's name, position and contact details	Description of the processing
Amazon Web Services EMEA SARL	38, avenue John F. Kennedy, 1855 Luxembourg	Provision of cloud hosting, communication and SSO services for the processor, including the cloud storage on which UMSaaS is hosted.
becker + brügesch Entsorgung GmbH	Warturmer Heerstr. 120 29197 Bremen	Provision of data media destruction services.
Citrix Systems UK Ltd	Building 3, Chalfont Park, Chalfont St Peter, Gerrards Cross, Buckinghamshire SL9 0BG, Great Britain.	Hosting of ShareFile accounts for the exchange of larger data packages, in particular used for the provision of support services by the processor.
Microsoft Ireland Operations, Ltd.	Attn: Data Privacy, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland	Various hosting, communication and SaaS services used for different business operations of the processor.
PLUTEX GmbH	Hermann-Ritter-Straße 108, 28197 Bremen, Germany	Provision of servers for the hosting of internal services of the processor.
ServiceNow Nederland B.V.	Attn: Legal Department, Hoekenrode 3, 1102 BR Amsterdam, Netherlands	Provision of the tools for customer support ticketing system and customer facing service interfaces.
TeamViewer GmbH	Bahnhofsplatz 2, 73033 Göppingen, Germany	Provision of communication and Desktop Sharing Services used for the support services provided by the processor to the controller.