Data Processing Agreement in acc. with Art. 28 General Data Protection Regulations (GDPR)

between

WIBU-SYSTEMS AG
Zimmerstr. 5
D-76137 Karlsruhe
Germany

(hereinafter: **Processor**)

and

.....

.....

.....

(hereinafter: **Client**)

1. Recital

The Processor conducts maintenance services on the IT systems operated by the Client. It cannot be excluded that the Processor will have access to or become aware of personal data in this context. The contracting parties agree that the Client alone will determine the purpose and means of the processing of such personal data in the provision of these services. The processing of such personal data is therefore to be carried out on behalf of the Client only in accordance with Art. 28 et seq. General Data Protection Regulations (hereinafter: "GDPR").

2. Scope and Term

2.1 The subject matter of this order processing agreement (hereinafter: "Agreement") results from the "Service Agreement" concluded between the Processor and the Client on the basis of the valid

- GTC Part C: Special provisions for hosting Services

and the respective supplementary product-specific hosting conditions:

- CodeMeter Cloud Hosting Conditions
- CodeMeter Cloud Lite Hosting Conditions
- CodeMeter Cloud FSB Hosting Conditions
- CodeMeter License Central Hosting Conditions
- CodeMeter License Portal Hosting Conditions

The agreement includes all of the service description of the corresponding aforementioned hosting conditions in which employees of the Processor or third parties commissioned by the Processor may come into contact with the Client's data.

2.2 The term of the Agreement is identical to the term of the Service Agreement.

3. Specification of the Processing

3.1 The type of the personal data and the categories of data subjects (Art. 28 (3) GDPR) are listed in **Annex 1**.

3.2 The contractually agreed data processing shall take place in the territory described in **Annex 3** for the respective product. If several possible territories are specified, it shall be agreed separately with the Client in which territory or territories its processing shall take place. The Processor shall inform the Client at least 30 calendar days in advance if the data processing is to be relocated to another member state of the European Union, to another state party to the Agreement on the European Economic Area or to a region outside the EEA. Any relocation to a third country requires the prior consent of the client and may only take place if the special requirements of Art. 44 et seq. GDPR are fulfilled.

3.3 The Client alone determines the purpose and means of the processing of personal data in the context of this Agreement and is therefore the data controller in accordance with Art. 4 (7) GDPR. As such, the Client is responsible for compliance with the GDPR as stipulated in Art. 24 GDPR.

4. Quality Assurance and Other Duties of the Processor

In addition to the provisions of this Agreement, the Processor shall comply with other legal obligations under Art. 28 to 33 GDPR. In particular, the Processor ensures compliance with the following requirements:

(a) The Processor has appointed a Data Protection Officer who executes his duties according to Art. 38 and 39 GDPR. The contact details of the data protection officer can be found in **Annex 4**. The Client will be notified immediately about any change of the appointed Data Protection Officer.

(b) Maintaining confidentiality in accordance with Art. 28 (3) S. 2 lit. b, 29, and 32 (4) GDPR during and after the contractual relationship between the Parties. The Processor will only assign members of staff for the execution of the agreed works who have been formally committed to confidentiality and who have been made aware of the relevant data protection regulations applicable to them. The Processor and any person reporting to the Processor who has access to personal data must only process the personal data in accordance with the Client's instructions, including the powers conferred to them by this Agreement, unless they are required to process this data by law.

(c) Implementing and maintaining all technical and organizational measures required for the data processing in accordance with Art. 28 (3) S. 2 lit. c and 32 GDPR and Sect. 5 of this Agreement.

(d) The Client and the Processor will cooperate with the supervisory authorities if requested in the performance of its obligations.

(e) Immediately notifying the Client about any investigatory or other activities by supervisory authorities in so far as they relate to this Agreement. This also applies if relevant authorities conduct investigations as part of administrative or criminal proceedings relating to the processing of personal data by the Processor. The Processor will remedy any deficiency identified in official inspection reports immediately.

(f) In so far as the Client is subject to investigations by supervisory authorities, administrative or criminal proceedings, liability claims from an affected person or third party, or other claims relating to the data processing within the context of this Agreement, the Processor will support the Client to the best of its ability.

(g) The Processor will regularly, but at least annually, control its internal processes and technical and organizational measures to ensure that the data processing within his responsibility is compliant with the current requirements and standards of data protection law and ensures due protection for the rights of the persons affected.

(h) Providing proof of the implemented technical and organizational measures to the Client in accordance with the Client's power of supervision arising from Sect. 6 of this Agreement.

(i) The Processor will not connect any hardware to the systems of the Client or install software thereon without the prior consent of the Client. The Processor must not process personal data under the Client's responsibility with the systems of third parties, including for purposes of testing.

(j) The Processor will notify the Client immediately, should personal data under the Client's responsibility be at risk at the Processor as a result of seizure or confiscation, insolvency or mediation proceedings, or other incidents or actions by third parties. The Processor will also inform all persons responsible in such events that the ownership of the data lies with the Client.

5. Technical and Organizational Measures

5.1 The Processor is required to ensure the security of processing in accordance with Art. 28 (3) lit. c and 32 GDPR, in particular in conjunction with Art. 5 (1) and (2) GDPR. The measures to be implemented generally represent measures to ensure data security and the provision of a level of security appropriate for the risks in terms of the confidentiality, integrity, availability, and resilience of the systems, with particular attention to the current state of technology, the cost of implementation, and the type, scope, circumstances, and purpose of the data processing as well as the varying likelihood and severity of the risks to the rights and freedoms of natural persons in accordance with Art. 32 (1) GDPR.

5.2 The Processor will arrange the internal organization in its sphere of responsibility in a way that satisfies the particular requirements of data protection regulations. It will implement the technical and organizational measures (hereinafter: TOM) detailed in **Annex 2** to ensure the appropriate security of all personal data that he has access to in the context of the services. If any of these TOM are changed, the Processor will adjust the statements in **Annex 2** accordingly and notify the Client by providing it with the updated document. The level of security ensured by the TOM detailed in **Annex 2** must be maintained.

5.3 The Client has taken note of the TOM detailed in **Annex 2**. They are considered part of the contractual basis for the data processing under the terms of this Agreement. The Parties agree to conduct any required inspections or audits by the Client by mutual consent.

5.4 The TOM are subject to technical developments and evolution. With this in mind, the Processor may implement alternative appropriate measures as long as these do not fall below the level of security ensured by the agreed TOM. Any substantial changes must be documented.

6. Client's Supervisory Rights

6.1 The Client may conduct inspections with the consent of the Processor or to commission external inspectors for individual inspections. It may ascertain whether the Processor complies with the requirements of this Agreement by means of random checks that are typically announced with at least 30 days notice and conducted during regular operating hours.

6.2 The Processor ensures that the Client can ascertain whether the Processor complies with his duties in accordance with Art. 28 GDPR. He supports the Client in the implementation of inspections and random checks. The Processor will provide the Client with the required information in text form within appropriate notice and, in particular, provide proof of the implementation of technical and organizational measures.

6.3 Proof of the implementation of measures affecting more than the concrete commission can be provided in the following forms:

(a) Compliance with agreed codes of conduct in accordance with Art. 40 GDPR;

(b) Certification by approved certification processes in accordance with Art. 42 GDPR;

(c) Current reports, statements, or excerpts thereof from independent entities (e.g. auditors, data protection officers, IT security teams, data protection auditors, quality auditors etc.); or

(d) Suitable certification in IT security or data protection audits (e.g. BSI – German Federal Office for Information Security baseline protection).

6.4 The Client will notify the Processor immediately and comprehensively about any mistakes or irregularities concerning data protection regulations identified when reviewing the delivered services.

7. Support for the Performance of the Client's Duties

7.1 The Processor supports the Client in the maintenance of the duties concerning the protection of personal data in accordance with Art. 30 to 36 GDPR, the duty to report any data incidents, the data protection impact assessments, and prior consultations.

7.2 This includes, but is not limited to:

(a) Maintaining an appropriate level of protection by means of technical and organizational measures in accordance with Sect. 5;

(b) Reporting any violation of data protection immediately to the Client;

(c) Supporting the Client in its duty to inform all persons affected and providing all relevant information in this context immediately;

(d) Supporting the Client with data protection impact assessments;

(e) Supporting the Client with creation of records of processing activities;

(f) Supporting the Client as part of prior consultations with supervisory authorities; and

(g) If possible, supporting the Client with technical and organizational measures for the client´s obligation to answer requests of persons affected according to Chapter 3 GDPR.

8. Authority of the Client

8.1 The Processor processes the personal data within the responsibility of the Client only as instructed by the Client and documents all instructions received from the Client. In particular the Processor must not remove, change, or delete any personal data without the Client's express consent. This applies irrespective of the form in which such data is recorded or stored.

8.2 The Client's authority as stipulated in Sect. 8.1 also covers instructions concerning the type, scope, and procedure of maintenance works to IT systems as part of the Service Agreement to the extent that these affect the processing of personal data.

8.3 The Processor will confirm oral instructions immediately at least in text form.

8.4 The Processor will notify the Client immediately about any instructions deemed by him to not comply with data protection requirements. The Processor is entitled to suspend the implementation of such instructions until they have been confirmed or revised by the Client.

8.5 The Client appoints a person to exercise his right to issue instructions. The Processor appoints a person to receive the instructions of the Client and ensure their implementation. These persons and their contact details are listed in **Annex 4**.

8.6 If the Processor is obliged by legal requirements to carry out further processing, it shall inform the Client thereof prior to the processing, unless the relevant law prohibits such notification due to an important public interest.

9. Remuneration

All services required by the GDPR (e.g. deletion, rectification, direct access) are already covered by the Service Agreement. The Client will pay the Processor for any additional support services that are not covered by the Service Agreement and not due to any wrongdoing on the part of the Processor. The Processor will submit to Client an offer for such services for Client´s approval.

10. Sub-Contracts

10.1 For the purposes of this Agreement, sub-contracts refer to all services that relate immediately to the delivery of the principal services. This does not include other services that the Processor uses, including, but not limited to telecommunication services, postal or other transport services, maintenance and user support services, storage device destruction services, or other measures to ensure the confidentiality, availability, integrity, and resilience of the hardware and software of data processing facilities. The Processor is required to implement appropriate agreements and controls in accordance with the legal requirements to protect the security and confidentiality of the Client's data when using sub-contracted services.

10.2 The Processor must commission services from sub-contractors (additional, subordinate processors) only with the prior express and written consent of the Client.

(a) The Client consents to the commissioning of the sub-contractors named in **Annex 3** on the condition of the presence of a written contractual agreement in accordance with Art. 28 (2 to 4) GDPR.

(b) The Client hereby provides the Processor with a written and general authorization to change the sub-contractor named in Sect. 10.2 a) of this Agreement if:

- The Processor gives the Client at least 30 days in advance prior notice of the commissioning to other sub-contractors in writing or text form, and
- The Client has not objected to the commissioning in writing or text form before the planned transfer of the data, and
- A written contractual agreement in accordance with Art. 28 (2 to 4) GDPR is implemented.

10.3 The transfer of personal data of the Client to a sub-contractor and the initiation of works by a sub-contractor are only permitted if all conditions for such sub-contracting are present and fulfilled. The Processor will provide the Client with a copy of the agreement entered into with the sub-contractor upon request by the Client.

10.4 Should the sub-contractor provide the agreed services outside of the member states of the EU / EEC, the Processor implements appropriate measures to ensure compliance with data protection law. This also applies if a service provider as according to Sect. 10.1 Sentence 2 is commissioned.

10.5 Any further sub-contracting by the sub-contractor requires the express written consent of the Processor. Any contractual requirements are to be imposed on all further parties in the sub-contracting chain. For this purpose, the technical and organizational measures agreed in particular with the sub-contractors must guarantee an equal or better level of security.

10.6 The Processor remains responsible for the activities assigned to sub-contractors to the same extent as if these were implemented by the Processor himself.

11. Correction, Restriction, and Deletion of Data

11.1 The Processor must not correct, delete, or otherwise restrict the use of the data made available to it for data processing, unless on the documented instruction of the Client. Should an affected person contact the Processor directly in this regard, the Processor will immediately notify the Client.

11.2 The rights stated in Chapter III GDPR for affected persons must be assured by the Client. The Processor will support the client, if possible, with suitable technical and organizational measures without additional costs.

11.3 No copies or duplicates of the data must be created without the knowledge of the Client. This does not include backup copies to the extent required to ensure orderly data processing as well as data required for compliance with the legal retention requirements.

12. Deletion and Return of Personal Data

12.1 After the completion of the contractually agreed works or earlier at the request of the Client – but no later than the termination of the Service Agreement – the Processor will:

(a) return all documents to the Client that have come into its possession, results of the processing and use of data, and data sets relating to the contractual relationship with the Client, or

(b) destroy them in accordance with the applicable data protection law with the Client's prior consent. The same applies to testing and waste materials. A record of the destruction is to be provided upon request.

12.2 All records to serve as proof of the contractually correct and orderly processing of the data are to be maintained by the Processor beyond the termination of the Agreement for the applicable retention periods. In order to satisfy this obligation, the Processor may transfer such records to the Client upon termination of this Agreement.

13. Liability

Liability for damages caused by data processing is governed by Art. 82 GDPR. Accordingly, the Processor is only liable for damages if he has not complied with the specific duties and responsibilities imposed on Data Processors by the GDPR or if he has acted in non-observance or in breach of instructions legitimately issued by the Client.

14. Final Clauses

14.1 Unless explicitly stated otherwise in this Agreement, the terms in this Agreement are to be interpreted in accordance to their definitions in the GDPR.

14.2 Any amendments or additions to this Agreement must be made in writing (including by telefax or email). This includes any waiver to this requirement of the written form.

14.3 This Agreement is subject to the laws of the Federal Republic of Germany. The exclusive jurisdiction and legal venue for disputes and place of delivery for all obligations arising from this Agreement is the registered seat of the Processor.

14.4 Should any one of the clauses of this Agreement be or become partially or fully void or invalid or there be any omissions in this Agreement, this shall not affect the validity of the remaining Agreement. The Parties agree to replace the void or invalid clause with a clause that is legally valid and comes closest to the original intent of the Parties. In the case of an omission, the Parties agree to find a stipulation that would have been agreed in accordance with the intention and purpose of this Agreement had the Parties considered the matter in question at the original conclusion of this Agreement.

14.5 The following annexes form part of this Agreement:

Annex	Title
Annex 1	Information about Data Processing
Annex 2	Technical and organizational measures
Annex 3	Sub-Contractors
Annex 4	Contact persons

..... (Place and Date)	Karlsruhe, 2024-09-03 (Place and Date)
..... (Client)	WIBU-SYSTEMS AG (Processor)
Represented by:	Represented by:
(Signature)	 (Signature)
..... (Name), (Function)	Dr. Peer Wichmann, Data Protection Officer
(Signature)	
..... (Name), (Function)	

Issue date: 2024-09-03

Annex 1: Information about the Data Processing

1. Types of Personal Data

Depending on the product used, different types or categories of data are subject to collection, processing, and use:

1.1 CodeMeter Cloud Hosting

The following types or categories of data are subject to collection, processing, and use:

☑ Personal Data	☐ Special Categories of Personal Data (cf. Art. 9 (1) GDPR)
User accounts	
Encrypted passwords	
Login records	
IP addresses of end users	
Serial numbers of CmCloud Containers	
Programmed licenses	
Browser identities	
Client computer name	

1.2 CodeMeter Cloud Lite Hosting

The following types or categories of data are subject to collection, processing, and use:

☑ Personal Data	☐ Special Categories of Personal Data (cf. Art. 9 (1) GDPR)
User accounts	
Login records	
IP addresses of end users	
Serial Numbers of CmContainers	
Programmed licenses	
Browser identities	
Client computer name	

1.3 CodeMeter Cloud FSB Hosting

The following types or categories of data are subject to collection, processing, and use:

☑ Personal Data	☐ Special Categories of Personal Data (cf. Art. 9 (1) GDPR)
User accounts	
Login records	
IP addresses of end users	
Serial numbers of CmCloud Containers	
FSB Contents	
Usage Data	
Browser identities	

1.4 CodeMeter License Central Hosting

The following types or categories of data are subject to collection, processing, and use:

☑ Personal Data	☐ Special Categories of Personal Data (cf. Art. 9 (1) GDPR)
User accounts	
Login records	
IP addresses of end users	
Serial numbers of CmContainers	
Programmed licenses	
Browser identities	
Client computer name	

1.5 CodeMeter License Portal Hosting

The following types or categories of data are subject to collection, processing, and use:

☑ Personal Data	☐ Special Categories of Personal Data (cf. Art. 9 (1) GDPR)
User accounts	
Login records	
IP addresses of end users	
Serial numbers of CmContainers	
Programmed licenses	
Browser identities	
Client computer name	

2. Categories of Affected Persons

The persons affected by the processing of the personal data include:

- Employees of the Processor
- Employees of the Client and of companies affiliated with the Client
- End users of the Client and of companies affiliated with the Client

Issue date: 2024-09-03

Annex 2: Technical and organizational measures

1. Confidentiality (Art. 32 (1) lit. b GDPR)

Physical access	Doors to the premises are kept closed.
	Electric door openers are installed.
	Access controls are in place to ensure that delivery people or other external persons, including service providers, only enter the premises when required and never unaccompanied.
	Keys are held by a closely defined group of authorized persons. All key holders know which measures need to be taken in the case of loss.
	A central locking system with separate locking areas is in place.
	Burglar alarms are active outside of business hours.
System access	Users logins to the operating systems are set with passwords.
	Only one login is used per user. Only special systems use group accounts. These are only available to a closely defined group of data center personnel.
	Passwords contain at least eight characters, including capitals, figures, and special characters.
	Password guidelines are in place.
	When users leave their work station, their computers are manually or automatically locked by a screen saver / lock after a defined period.
Data access	Users are assigned to separate user groups with separate rights to access data. An entitlement concept is in place.
	User logins and logouts are recorded (with statistical analysis).
	Passwords must not be shared with colleagues (cf. password guidelines).
	All changes and deletions are recorded.
Separation	Any changes are introduced in a "test – demo – live" process whenever possible on the Client's systems.
	Physical separation of data is ensured.
	Data is deleted on the instructions of the Client.
Destruction of data media	The destruction of data media is effected according to ISO/IEC 21964-1:2018.

2. Integrity (Art. 32 (1) lit. b GDPR)

Data communication	Open-VPN, IPSEC are used.
	A log file is created.
Entries	A log file records login attempts, logouts, and password changes.

3. Availability and Resilience (Art. 32 (1) lit. b GDPR)

Availability	Uninterruptible power supply systems are used.
	The systems are protected externally by means of a firewall.
	All computers use current anti-virus software.
	Regular backups (incremental and complete) are conducted on a set cycle.
	The systems are equipped with redundant hard-drive systems (RAID-1, RAID-5).
	The data centers are climate controlled.
	Security guidelines are in place.
Security Updates	Available security updates are implemented automatically at regular intervals.
Quick Recovery	The systems are equipped with redundant hard-drive systems (RAID-1, RAID-5).
Storage of backup media	Backup media are stored and locked in a fire section separated from the server room.
Fire protection	The server room used for hosting is equipped with an automatic fire extinguishing system.

4. Regular Testing, Assessment, and Evaluation Procedures (Art. 32 (1) lit. d, and 25 (1) GDPR)

Order Monitoring	No data processing in accordance with Art. 28 GDPR without relevant instructions of the Client: IT management is in charge of monitoring the technical and organizational requirements defined by the Agreement.

Issue date: 2024-09-03

Annex 3: Sub-Contractors

Wibu-Systems operates data centers in the following regions:

Sub-Contractor	Address	Service	Service location	CodeMeter Cloud	CodeMeter Cloud Lite	CodeMeter Cloud FSB	CodeMeter License Central	CodeMeter License Portal
Claranet GmbH	Hanauer Landstrasse 196 D-60314 Frankfurt am Main Germany	Data center operations	Germany		✓		✓	✓
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy 1855 Luxembourg	Data center operations	Germany, Japan, USA	✓		✓		

Issue date: 2024-09-03

Annex 4: Contact Persons

Authorized Representatives of the Client:

Name	
Address	
Phone	
Email	

Recipient of Instructions to the Processor:

Name	Uwe Traschütz, Director Wibu Operating Services (WOPS)
Address	Zimmerstr. 5, D-76137 Karlsruhe, Germany
Phone	+49 721 93172-312
Email	uwe.traschuetz@wibu.com

Data protection Officer of the Processor:

Name	Dr. Peer Wichmann
Address	Zimmerstr. 5, D-76137 Karlsruhe, Germany
Phone	+49 721 93172-0
Email	dataprotection@wibu.com

Issue date: 2024-09-03