Data Processing Agreement (DPA) pursuant to Art. 28 (3) GDPR

between

Company .....

Address .....

Zip code and City .....

Country .....

as Controller pursuant to Art. 4 Nr. 7 GDPR („**Client**")

And

WIBU-SYSTEMS AG
Zimmerstraße 5
76137 Karlsruhe
Germany

as Processor pursuant to Art. 4 Nr. 8 GDPR („**Processor**")

§1 Subject matter of the contract

1.1 The Processor operates IT systems for the Client in accordance with the individual contract. In doing so, the Processor gains access to personal data and processes this data exclusively on behalf of and in accordance with the instructions of the Client.

1.2 The following annexes form part of the contract:

Annex	Designation
Annex 1	Information on Data Processing: 1.1 CodeMeter Cloud Hosting 1.2 CodeMeter Cloud Lite Hosting 1.3 CodeMeter Cloud FSB Hosting 1.4 CodeMeter License Central Hosting/Remote Maintenance 1.5 CodeMeter License Portal Hosting/Remote Maintenance 1.6 CodeMeter License-as-a-Service 1.7 CodeMeter License Reporting Hosting
Annex 2	Technical and Organizational Measures
Annex 3	Subcontractors
Annex 4	Contact persons

1.3 The scope and purpose of data processing by the Processor are set out in the individual contract. The Client is solely responsible for assessing the permissibility of data processing in accordance with Art. 6 (1) GDPR.

1.4 The parties enter into this contract to specify their mutual rights and obligations under data protection law. In the event of any conflict, its provisions shall take precedence over those of the individual contract.

1.5 The provisions of this contract apply to all activities related to the individual contract in which the Processor and its employees or agents come into contact with personal data originating from the Client or collected for the Client or otherwise processed on its behalf.

1.6 The term of this contract is based on the term of the individual contract, unless the following provisions give rise to further obligations or rights of termination.

1.7 The contractually agreed data processing shall be carried out in the countries described in **Annex 3** for the respective product. If several countries are specified, the individual contract shall stipulate in which country or countries the processing shall take place. If personal data is transferred to subcontractors outside the EU or the EEA, they must first commit to complying with the standard contractual clauses in accordance with Commission Implementing Decision (EU) 2021/914 of June 4, 2021, thereby ensuring an adequate level of data protection within the meaning of Art. 46 (2) (c) GDPR. In the case of subcontractors based in the United States, the Processor has verified in advance that they are a certified organization in accordance with Commission Implementing Decision (EU) 2023/1795 of July 10, 2023.

§2 Purpose of processing, type of data processed, and categories of data subjects

The purpose of processing, the type of data processed, and the categories of data subjects are set out in **Annex 1**, depending on the conditions applicable under the individual contract.

§3 Client's right to issue instructions

3.1 The Processor may only collect, use, or otherwise process data within the scope of the individual contract and in accordance with the Client's instructions; this applies in particular to the transfer of personal data to a third country or to an international organization. If the Processor is obliged to carry out further processing under European Union law or the law of the member states to which it is subject, it shall inform the Client of these legal requirements prior to processing.

3.2 The Client's instructions are initially set out in this contract and may subsequently be amended, supplemented, or replaced by the Client through individual instructions. The authorized contact persons for both parties are listed in **Annex 4**. Any changes must be taken into account promptly.

3.3 All instructions issued shall be documented by both the Client and the Processor and shall be retained for the duration of their validity and for a further calendar year thereafter.

3.4 If the Processor believes that any instruction from the Client violates data protection regulations, it shall immediately notify the Client. The Processor is entitled to suspend the execution of the instruction in question until it has been confirmed or amended by the Client. The Processor may refuse to execute an instruction that is obviously unlawful.

3.5 If an instruction from the Client increases the effort required by the Processor to perform a service owed under the individual contract, the Processor may demand a corresponding adjustment to the agreed remuneration. The Processor must inform the Client of the additional costs before performing the service.

3.6 To the extent that the Processor is prevented from performing a service owed under the individual contract due to an instruction from the Client, the Processor shall be released from its performance obligations. The Processor's claim to the agreed remuneration shall remain unaffected by this.

§4 General obligations of the Processor

4.1 The Processor is obliged to observe the statutory provisions on data protection and not to pass on or to grant access to third parties to information obtained from the Client's sphere. The Processor shall implement appropriate technical and organizational measures, consistent with industry standards, to protect all documents and data from unauthorized access.

4.2 The Processor shall organize its internal operations within its area of responsibility in such a way that they meet the specific requirements of data protection. The Processor guarantees that it has taken all necessary technical and organizational measures (TOMs) to adequately protect the Client's data in accordance with Art. 32 GDPR **(Annex 2)**. With regard to the protection purposes of the data processed on its behalf, the Client has reviewed the Processor's technical and organizational measures prior to concluding the contract and has assessed them as sufficient.

4.3 The technical and organizational measures are subject to technical progress and further development. The Processor is entitled to adapt measures to technical and organizational developments, provided that these do not fall short of the agreed standards. Significant changes must be documented and made available to the Client immediately in a new version as an annex.

4.4 The Processor shall regularly, at least once a year, review its internal processes and technical and organizational measures to ensure that processing within its area of responsibility complies with applicable data protection laws and that the rights of data subjects are protected.

4.5 The contact persons appointed for data protection are listed in **Annex 4**. Changes to this information shall be communicated to the Client without delay.

4.6 Any person employed in data processing by the Processor are prohibited from collecting, using, or otherwise processing personal data without authorization. This also applies to the use of anonymized data. The Processor shall impose corresponding obligations on all persons entrusted by it with the processing and fulfillment of this contract (confidentiality obligation, Art. 28 (3) (b) GDPR) and instruct them on the specific data protection obligations arising from this contract and the existing obligation to follow instructions and purpose limitation and shall ensure compliance with the aforementioned obligation with due care.

§5 Processor's information obligations

5.1 In the event of disruptions, suspected data protection violations or violations of the Processor's contractual obligations, suspected security-related incidents or other irregularities in the processing of personal data, the Processor shall inform the Client immediately.

5.2 The Processor shall immediately take the necessary measures to secure the data and mitigate any possible adverse consequences for the data subject(s), inform the Client thereof, and request further instructions from the Client.

5.3 Upon request, the Processor shall support the Client in fulfilling the requests and claims of data subjects in accordance with Art. 12 ff. GDPR and in complying with the obligations set out in Art. 32 to 36 GDPR within the scope of its abilities and to a reasonable extent. The Processor shall provide additional support services only if the Client bears the associated costs.

5.4 If the Client's data held by the Processor is at risk due to seizure or confiscation, insolvency or composition proceedings, or other events or measures taken by third parties, the Processor shall inform the Client immediately, unless prohibited from doing so by court or official order. In this context, the Processor shall immediately inform all competent authorities that the Client has sole decision-making authority over the data.

5.5 The Processor and, where applicable, its representatives shall maintain a record of all categories of processing activities carried out on behalf of the Client, containing all information specified in Art. 30 (2) GDPR. The record shall be made available to the Client upon request.

§6 Control rights of the Client

6.1 The Processor shall demonstrate compliance with the obligations set out in this contract to the Client upon request by appropriate means.

6.2 If inspections by the Client or an auditor commissioned by the Client are necessary in individual cases, these shall be carried out during normal business hours without disrupting operations. The parties shall mutually agree on the timing and scope of the inspection, with the inspection being scheduled at least 30 calendar days in advance.

6.3 The Processor shall only allow persons who are subject to confidentiality obligations to carry out the inspection, in particular with regard to information about the Processor's trade secrets, its operations and equipment, data of other customers, and existing security measures. If the inspection is not carried out by a person already known to the Processor, the inspector must prove their legitimacy to the Client at least ten calendar days before the inspection is carried out. The Processor is not obliged to accept an inspector who is in competition with the Processor.

6.4 The Client shall document the results of the inspection and communicate them to the Processor. If the Client discovers any errors or irregularities, particularly when checking data processing results, it shall inform the Processor immediately. If the inspection reveals circumstances that require changes to the prescribed procedure in order to be avoided in future, the Client shall immediately inform the Processor of the necessary procedural changes.

§ 7 Use of additional processors (subcontractors)

7.1 Within the scope of its contractual obligations, the Processor is authorized to establish further contract processing relationships with subcontractors. The Processor shall carefully select subcontractors based on their suitability and reliability. The Processor shall oblige them to comply with the provisions of this contract and shall ensure that the Client can exercise its rights under this contract, in particular its rights of inspection and control. Upon request, the Processor shall provide the Client with evidence of the conclusion of agreements with its subcontractors regarding data processing.

7.2 The subcontractors currently working for the Processor in accordance with para. 7.1 are listed in **Annex 3**. For these subcontractors, consent to act as additional processors is deemed to have been given upon commissioning of the individual contract; the Processor shall notify the Client of any changes in a timely manner.

7.3 If the Processor subsequently engages additional processors, the Client may object within one month of the subcontractors being listed in **Annex 3** if there is a legitimate data protection concern that would prevent the subcontractors from being engaged.

7.4 A subcontractors relationship within the meaning of the above provisions does not exist if the Processor commissions third parties to provide services that are to be regarded as purely ancillary services. These include, for example, postal, transport and shipping services, security and cleaning services, and telecommunications services without any specific connection to services that the Processor provides for the Client.

§8 Inquiries and rights of data subjects

8.1 If a data subject asserts rights, such as the right to information, correction, or deletion of their data, directly against the Processor, the Processor shall forward the request to the Client without delay, provided that it is possible to match it to the Client according to the information provided by the data subject. The Processor shall not be liable if the Client does not respond to the data subject's request or does not respond correctly or in a timely manner.

8.2 The Client and the Processor shall cooperate with the supervisory authority in the performance of its tasks upon request.

§9 Liability

9.1 The Processor shall be liable to data subjects in accordance with Art. 82 GDPR.

9.2 The Processor's liability to the Client for breach of obligations under this contract shall be governed by § A7 of the Processor's General Terms and Conditions.

§10 Termination of the individual contract and this contract

10.1 The term of this contract is governed by the individual contract. The mutual right to extraordinary termination of this contract for good cause remains unaffected. Good cause for the Client shall include, in particular, the Processor's violation of a provision of the GDPR or this contract with at least gross negligence.

10.2 After termination of the individual contract, this contract shall remain valid for as long as the Processor holds personal data that was provided to it by the Client or that it has collected on behalf of the Client. Upon termination of this contract by way of extraordinary termination, the individual contract shall also terminate if it requires the processing of personal data.

10.3 Upon termination of the individual contract or at any time upon request, the Processor shall return all documents, data, and data carriers provided to it to the Client or delete them at the Client's request, unless there is an obligation to store the personal data under Union law or the law of the Federal Republic of Germany. The Processor shall provide documentary evidence of proper deletion at the Client's request.

§11 Final provisions

11.1 Declarations between the parties must be made in writing, whereby email is sufficient.

11.2 The contract is subject to German law.

11.3 The place of performance and jurisdiction for all disputes arising from and in connection with this contract shall be determined by the individual contract.

11.4 Should any of the above provisions be or become invalid or should a necessary provision not be included, this shall not affect the validity of the remaining provisions. In this case, the parties shall endeavor to find a mutually acceptable solution.

..... (Place, date)	Karlsruhe, on ..... (Place, date)
..... (Client)	WIBU-SYSTEMS AG (Processor)
by:	by: Sven Maier — Signed by: Sven Maier — Date: 2026-01-29 11:16:59 CET
(Signature)	(Signature)
..... (Name), (Position)	Dr. Sven Maier, Data Protection Officer
(Signature)	
..... (Name), (Position)	

Stand: 2026-02-01

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

☑ 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

☑ 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

☑ 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/Remote Maintenance

☑ 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/Remote Maintenance

☑ 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	

1.6 CodeMeter License-as-a-Service

☑ 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 CmContainers	
Programmed licenses	
Usage Data	
Browser identities	
Client computer name	

1.7 CodeMeter License Reporting Hosting

☑ 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 CmContainers	
Programmed licenses	
Usage Data	
Browser identities	
Handles of the License Usage	
ProductCode	
FeatureCode	
ReleaseCode	
ProductItemID	
EPD 136 (TicketLicenseID)	

2. Categories of Affected Persons

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

- Employees of the Processor and of the Processor's sales partners
- Employees of the Client and of companies affiliated with the Client
- End users of the Client and of companies affiliated with the Client

Annex 1: Information about the Data Processing

3. Processing Purpose

Depending on the product in use, the processing purposes vary. These are specified as follows for each individual:

3.1 **CodeMeter Cloud Hosting**
Providing a trust anchor (dongle) in the cloud. This processing enables the operator to manage cloud containers and allows end-users to utilize the containers, particularly for cryptographic services.

3.2 **CodeMeter Cloud Lite Hosting**
Providing licenses for user programs. Management is conducted via the License Central service. License retrieval by the end-customer can be realized through Cloud Lite.

3.3 **CodeMeter Cloud FSB Hosting**
This is a special case of cloud hosting. It offers a trust anchor that allows the licensor to create licenses. The licensor can edit the trust anchor's options and logs. End-customer access typically does not exist.

3.4 **CodeMeter License Central Hosting/Remote Maintenance**
Managing end-customer licenses by the licensor. Licenses are automatically deployed to the end-customer.

3.5 **CodeMeter License Portal Hosting/Remote Maintenance**
This complements License Central and enables customized and unified license retrieval by the end-customer.

3.6 **CodeMeter License-as-a-Service**
License-as-a-Service is an easy-to-understand service for the creation, management, and distribution of licenses by the licensor and for the retrieval of licenses by the end customer. The service is based on the products CodeMeter License Central and CodeMeter License Portal.

3.7 **CodeMeter License Reporting**
Capturing, storing, and analyzing license usage data to provide the client with usage-based re-ports and dashboards for billing purposes, product improvement, and license/resource planning.

Issue date: 2026-02-01

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.
Remote Maintenance	Individual accounts where possible, passwords for group accounts are stored in encrypted form in a password manager.

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.
Login Data for Remote Maintenance	Storage of the encrypted password manager database on a secured server with access control and regular backups.

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: 2026-02-01

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	CodeMeter License-as-a-Service	CodeMeter License Reporting
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	✓		✓	✓	✓	✓	
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855, Luxembourg	Data-center operations	Germany							✓
Alibaba Cloud Computing Ltd.	Room 1-2-A06, Yungu Park, No. 1008 Dengcai Street, Sandun Town, Xihu District, Hangzhou City, Zhejiang Province	Data center operations	China	✓		✓	✓	✓	✓	

Issue date: 2026-02-01

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. Sven Maier
Address	Zimmerstr. 5, D-76137 Karlsruhe, Germany
Phone	+49 721 93172-0
Email	dataprotection@wibu.com

Issue date: 2026-02-01