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

Between

WIBU-SYSTEMS AG
Zimmerstrasse 5
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 determines 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 only on behalf of the Client 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/Remote Maintenance Conditions
- CodeMeter License Portal Hosting/Remote Maintenance Conditions
- CodeMeter License-as-a-Service
- CodeMeter License Reporting Condition

The Agreement covers all activities defined in the service specifications of the Service Agreement, in the provision of which personnel employed by the Processor or third parties commissioned by the Processor come into contact with any data of the Client.

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

3. Definitions

3.1 "Client Data" shall mean all information processed for Client by Processor including but not limited to Personal Data.

3.2 "Data Protection Laws" shall mean any laws that apply to the Processing of data by Processor under the Agreement. This includes laws, regulations, guidelines, requirements, and government issued rules in the U.S. and other jurisdictions, at the international, country, state/provincial, or local levels, currently in effect and as they become effective, including without limitation EU Directive 95/46/EC, the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**"), the UK Data Protection Act, 2018, the California Consumer Privacy Act of 2018 ("**CCPA**") as amended by the California Privacy Rights Act of 2020 ("**CPRA**"), the Virginia Consumer Data Protection Act ("**VCDPA**"), the Colorado Privacy Act ("**CPA**"), the Utah Consumer Privacy Act ("**UCPA**"), the Connecticut Data Privacy Act ("**CDPA**"), the New York SHIELD Act, and any applicable data security and/or privacy laws of other jurisdictions.

3.3 "Data Subject" shall mean any identified or identifiable natural person to whom Personal Data relates or identifies.

3.4 "Data Subject Request" shall mean a request to access, correct, amend, transfer, rectify, restrict, limit the use, opt out of sale or sharing or other processing, or delete Data Subject's Personal Data consistent with that person's rights under Data Protection Laws.

3.5 "De-Identified Data" shall mean information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, provided that the business possesses the information.

3.6 "Personal Data," "Personal Information," shall mean information that is linked, reasonably linkable, or relates to an identified or identifiable natural person. Both Personal Data and Personal Information are referred to in this Addendum as "Personal Data".

3.7 "Process" or "Processing" shall mean any operation or set of operations performed on Client Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, modification, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, sale, analysis, alignment or combination, restriction, erasure or destruction.

3.8 "Pseudonymous Data" shall mean Personal Data that cannot be attributed to a specific individual without the use of additional information, provided such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the Personal Data is not attributed to an identified or identifiable individual.

3.9 "Security Incident" shall mean any actual or suspected (after reasonable investigation) accidental, unauthorized, unintended, or unlawful processing, access to, exfiltration, theft, disclosure, destruction, loss, alteration, compromise, and/or malicious infection of Client Data transferred, transmitted, stored, or otherwise processed by Processor or any of its Sub-Processors or third parties that process Client Data on Processor's behalf.

3.10 "Sell" shall have the meaning as set forth in the Data Protection Laws.

3.11 "Sensitive Personal Information" shall have the meaning(s) provided in the Data Protection Laws.

3.12 "Services" shall have the same meaning provided under the Service Agreement.

3.13 "Share" shall have the meaning as set forth in the Data Protection Laws.

3.14 "Standard Contractual Clauses" shall mean the agreement executed by and between Client and Processor and attached hereto as Exhibit B pursuant to the European Commission's decision ((EU) 2021/914) of 4 June 2021 on Standard Contractual Clauses for the transfer of personal data to Processors established in countries outside the purview of the Client and Processor which do not ensure an adequate level of data protection.

3.15 "Sub-Processor" shall mean a Sub-Contractor engaged by Processor or its affiliates to Process Client Data as part of the performance of the Services.

3.16 "UK Addendum" shall mean the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, Version B1.0, attached hereto as Exhibit C.

4. Specification of the Processing

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

4.2 Client instructs Processor to Process Client Personal Data to perform the Services as described in this Agreement and the Service Agreement.

4.3 Processor shall only Process (including but not limited to Sale, Sharing, or Disclosure) Client Personal Data for the purposes of providing the Services specified in the Service Agreement and only in accordance with Client's documented instructions, which may be specific instructions or standing instructions of general application in relation to the performance of Processor's obligations under this Agreement, unless otherwise required under Data Protection Laws to which Processor is subject, in which case Processor shall notify Client prior to such Processing unless prohibited by law.

(a) Processor will not Sell or Share Client Personal Data, nor will it retain, use, or disclose Client Personal Data for any purpose other than for the specific business purpose of performing the Services specified in the Service Agreement. Processor will not Process Client Personal Data outside the direct business relationship between Client and Processor, including retaining, using, or disclosing Client Personal Data for a commercial purpose other than providing the Services specified in the Service Agreement or as required by law.

(b) Processor shall not aggregate, anonymize, or otherwise de-identify Personal Data without the prior written authorization of Client except as needed to perform the Services.

(c) Processor shall not combine Client Personal Data received from Client with any other information Processor receives from or on behalf of another person or business or which it collects from its own interactions with Data Subjects.

(d) Processor shall Process Personal Data under the Service Agreement in compliance with Data Protection Laws, including providing the same level of privacy protection required by Data Protection Laws. Processor will notify Client if Processor determines it its Sub-Processor(s) cannot meet its obligations under the Data Protection Laws, in which case Client may, upon thirty (30) days' notice, take reasonable and appropriate steps to stop and remediate unauthorized processing of Personal Data.

4.4 Processor shall maintain a record of all categories of Processing activities carried out on behalf of Client, including at least:

(a) The name and contact details of the Processor or Processors and of each Controller on behalf of which the Processor is acting, and, where applicable, of the Processor's and Controller's representatives, and the Data Protection Officers;

(b) The categories of Processing carried out on behalf of Client;

(c) The categories of Data Subjects whose Personal Data is Processed by Processor on behalf of Client;

(d) The categories of Personal Data Processed by Processor on behalf of Client;

(e) Where applicable, transfers of Personal Data to a country outside the European Economic Area, including the identification of the destination country and documentation of suitable safeguards pursuant to Section 6 of this DPA; and

(f) A general description of the technical and organizational measures implemented and maintained by the Processor to protect Client.

4.5 Processor shall be responsible for its compliance with all laws regarding data that cannot reasonably identify, be related to, describe, be capable of being associated with or be linked directly or indirectly to a Data Subject. To the extent Processor Processes De-Identified Data under the Agreement, Processor:

(a) Will not attempt to associate De-Identified Data with an individual;

(b) Will not attempt to re-identify De-Identified Data;

(c) Will maintain and use De-Identified Data only in a de-identified fashion; and

(d) Will not use De-Identified Data to infer information about, or otherwise link to, an identified or identifiable individual or a device linked to such an individual.

4.6 To the extent Processor Processes Pseudonymous Data under the Agreement, Processor will not attribute or attempt to attribute Pseudonymous Data to an identified or identifiable individual. Processor will ensure and provide documentation to Client to demonstrate that any information necessary to identify the Data Subject is:

(a) Kept separately from Pseudonymous Data; and

(b) Subject to effective technical and organizational controls that prevent access to such information.

4.7 Processor agrees to treat all Personal Data as confidential and will inform all individuals with authorized access to Personal Data of the confidential nature of such information. Processor will ensure that all employees are subject to binding confidentiality obligations.

4.8 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 country outside the list in **Annex 3** requires the prior consent of the Client and may only take place if the special requirements of Art. 44 et seq. GDPR are fulfilled.

4.9 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.

5. Quality Assurance and Other Duties of the Processor

5.1 In addition to the stipulations of this Agreement, the Processor has other legal duties 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 its 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 fulfillment of their responsibilities.

(e) Immediate notification to the Client about any investigatory or other activities of the 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 failings 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 control its internal processes and technical and organizational measures to ensure that the data Processing within its responsibility is compliant with the current requirements and standards of data protection legislation 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 does not have the right to 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.

6. Technical and Organizational Measures

6.1 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.

6.2 The Processor will arrange the internal organization in its area of responsibility in a way that satisfies the particular requirements of data protection regulations. He 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 them with the updated document. The level of security ensured by the TOM detailed in **Annex 2** must be maintained and must be tested, reviewed, and updated regularly. Should any of Processor's regular tests reveal that its policies and/or procedures to address the data security measures identified in **Exhibit B** and/or Article 32 of the GDPR do not adequately protect Client Data, Processor agrees to notify Client immediately.

6.3 The Client has checked and accepted the TOM detailed in **Annex 2**. They are considered part of the contractual basis for data Processing. The Parties agree to conduct any required inspections or audits by the Client by mutual consent.

6.4 The TOM are subject to technical developments and evolution. With this in mind, the Processor has the right to 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.

7. Client's Supervisory Rights

7.1 The Client is entitled to conduct inspections with the consent of the Processor or to commission external inspectors for individual inspections. Client has the right to 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.

7.2 The Processor agrees to allow for and contribute to reasonable audits by Client (or Client's designated auditor) to demonstrate Processor's compliance with its obligations under this Agreement and under Data Protection Laws ("Audits").

(a) Client may audit Processor's compliance with its obligations under this Agreement and Data Protection Laws, including but not limited to ongoing manual reviews, automated scans, regular assessments, audits, or other technical and operational testing at least once every 12 months.

(b) Client may use a third party to perform the Audit on its behalf, provided the third party is a qualified auditor and executes a confidential agreement acceptable to Processor before the Audit.

(c) Alternatively, subject to the prior written consent of Client, Processor may arrange for a qualified and independent auditor approved by Client to conduct, at least annually and at the Processor's expense, an audit of the Processor's policies and technical and organizational measures in support of its obligations under this Agreement and Data Protection Laws. Such audit shall be conducted using an appropriate and accepted control standard or framework and audit procedure, which must be approved by Client.

(d) Processor must provide Client with any Audit reports or findings generated in connection with any Audit at no charge, unless prohibited by law.

7.3 The Processor ensures that the Client can ascertain whether the Processor complies with its duties in accordance with Art. 28 GDPR. The Processor 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.

7.4 Proof of the implementation of such technical and organizational measures may include, but are not limited to, 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).

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

7.6 Processor shall notify Client without undue delay, and in no event later than 36 hours, after becoming aware of a Security Incident and shall co-operate with Client and take such reasonable commercial steps as are directed by Client to assist in the investigation, mitigation, and remediation of a Security Incident. Processor shall also provide Client with the assistance necessary for Client to meet its obligations relating to Security Incidents.

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

8.1 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. 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; and

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

8.2 Processor will provide such assistance, including taking any appropriate technical and organizational measures, as Client requests to help Client fulfill its obligations under Data Protection Laws to respond to Data Subject Requests. Notwithstanding its obligations under this Section, Processor is not obligated to respond to a Data Subject Request directly from a Data Subject and does not otherwise assume any liability or responsibility for responding to Data Subject Requests.

(a) Unless expressly authorized by Client, Processor shall not respond to any Data Subject Request.

(b) Unless it is permitted to retain Personal Data under the Data Protection Laws, Processor will comply with Client's direction to delete any Personal Data Processed under the Agreement and shall notify any Sub-Processors of such direction as applicable. Processor shall not be required to delete any of the Personal Data to comply with a Data Subject's request directed by Client if it is necessary to maintain such information in accordance with applicable law, in which case Processor shall promptly inform Client of the exceptions relied upon under applicable law and Processor shall not use the Personal Data retained for any other purpose than provided for by that exception.

(c) Processor will assist Client in complying with a Data Subject's request to limit the use and disclosure of Sensitive Personal Information and will not use the Sensitive Personal Information after it has received instructions from the Client and to the extent it has actual knowledge that the Personal Data is Sensitive Personal Information for any other purpose.

8.3 Both Parties will assist the other in communicating and cooperating with any regulators relating to Client Personal Data.

(a) Processor shall notify Client of all enquiries from a regulator that Processor receives which relate to the Processing of Personal Data under the Agreement, the provision or receipt of the Services, or either Party's obligations under the Agreement, unless prohibited from doing so by law or by the regulator.

(b) Unless a regulator requests in writing to engage directly with Processor, the Parties (acting reasonably and taking into account the subject matter of the request) agree that Client shall be responsible for handling all regulator requests. Client shall: (a) be responsible for all communications or correspondence with the regulator in relation to the Processing of Personal Data and the provision or receipt of the Services, and (b) keep Processor informed of such communications or correspondence to the extent permitted by law. Processor shall provide such assistance as Client may request in relation to such a regulator request.

8.4 If Client Personal Data is being provided to a third party in response to a subpoena or other discovery request, to the extent permitted by applicable law, Processor will provide Client with notice of the subpoena or discovery request prior to disclosing the Client Personal Data so that Client may, at its expense, object to the subpoena or discovery request, or seek an appropriate protective order.

9. Authority of the Client

9.1 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.

9.2 The Client's authority as stipulated in Sect. 9.1 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.

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

9.4 The Processor will notify the Client immediately about any instructions deemed by them 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.

9.5 The Client appoints a person to exercise its 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**.

9.6 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.

10. 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 present an offer for such services.

11. Sub-Contracts

11.1 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, or storage device destruction services. 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 subcontracted services.

11.2 The Processor must only commission services from Sub-Contractors (additional, subordinate Processors) 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 issues 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 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.

11.3 The transfer of personal data of the Client to a Sub-Contractor and the initiation of works by a Sub-Contractor are only allowed 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.

11.4 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 regulations. This also applies if a Processor as according to Sect. 11.1 Sentence 2 is commissioned.

11.5 Processor will ensure that any Sub-Processor that has access to Client Personal Data enters into a written agreement obligating the Sub-Processor to comply with terms that are at least as restrictive as those imposed on Processor under this DPA.

11.6 Processor shall remain fully liable to Client for the performance of its Sub-Processors' obligations and shall be responsible to Client for its Sub-Processors' Processing of Personal Data.

12. Correction, Restriction, and Deletion of Data

12.1 The Processor must not correct, delete, or otherwise restrict the use of the data made available to them 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.

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

12.3 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.

13. Deletion and Return of Personal Data

13.1 After the completion of the contractually agreed works or earlier at the request of the Client – but latest upon termination of the Service Agreement – the Processor will 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 destroy them in accordance with the applicable data protection regulations 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.

13.2 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 in accordance with the applicable retention periods. For its relief, the Processor can transfer such records to the Client upon termination of the Agreement.

14. Data Transfers

14.1 Processor will not transfer, Process, or cause another party to Process Client Data to or within any country outside of the European Economic Area without the consent of Client.

14.2 The Parties agree that the Standard Contractual Clauses, attached as **Exhibit D**, will apply to transfers of Personal Data either directly from the European Economic Area ("EEA") or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for Personal Data (a "Restricted Transfer") and to any other transfer which is a Restricted Transfer under the GDPR, and the Parties hereby enter into those Standard Contractual Clauses as a separate agreement in respect of such Restricted Transfer. For the avoidance of doubt, the Standard Contractual Clauses shall come into effect under this Section 14.2 on the later of (i) Client becoming a party to them by signing this Agreement; (ii) Processor becoming a party to them by signing this Agreement; or (iii) commencement of the relevant Restricted Transfer. If the Standard Contractual Clauses are invalidated or modified by judicial proceeding, statute, regulation, or otherwise, the Parties shall cooperate to identify alternative data transfer mechanisms, if available, provided that either Party may decline to adopt such mechanisms or to accept a modification of the Standard Contractual Clauses in its sole discretion.

14.3 The Parties agree that the UK Addendum to the Standard Contractual Clauses ("UK Addendum") will apply to transfers of Personal Data in Section 14.2, where the Personal Data will be transferred either directly from the United Kingdom ("UK") or via onward transfer to any country not recognized by the European Commission as providing an adequate level of protection for personal data (as described by the UK GDPR) (a "UK Restricted Transfer"), and the Parties hereby enter into the UK Addendum as a separate agreement in respect of the UK Restricted Transfer. For the avoidance of doubt, the UK Addendum shall come into effect under this Section 14.3 on the later of (i) Client becoming a party to it by signing this Agreement; (ii) Processor becoming a party to it by signing this Agreement; or (iii) commencement of the relevant UK Restricted Transfer. If the UK Addendum is invalidated or modified by judicial proceeding, statute, regulation, or otherwise, the Parties shall cooperate to identify alternative data transfer mechanisms, if available, provided that either Party may decline to adopt such mechanisms or to accept a modification of the UK Addendum in its sole discretion.

15. Additional Compliance Provisions

The Parties each represent and warrant to each other that they have read and understood the requirements of all applicable Data Protection Laws and will be responsible for their own compliance with them.

15.1 In addition to the terms set forth in Section 7.1 of this Agreement, Processor agrees, upon the reasonable request of Client, to make available to Client all information in its possession necessary to demonstrate Processor's compliance with its obligations under this Agreement and the Data Protection Laws. Client shall have the right to take reasonable and appropriate steps to ensure that the Processor is using Client Data in a manner consistent with Processor's obligations under this Agreement and Data Protection Laws.

15.2 The disclosure of Client Personal Data to Processor does not constitute a Sale or Sharing under the Data Protection Laws. Notwithstanding anything in the Agreement, the Parties acknowledge and agree that Client's provision of access to Personal Data is not part of and is explicitly excluded from the exchange of consideration or any other thing of value between the Parties.

15.3 This Agreement and the Hosting Agreement shall be interpreted as broadly as necessary to implement and comply with the mandatory provisions of the Data Protection Laws.

15.4 Each Party agrees that it is responsible for its own compliance with the requirements of the applicable Data Protection Laws and agrees to indemnify, defend, and hold harmless the other Party from and against any claims, demands, losses, liabilities, fines, penalties, costs, and expenses arising out of or relating to its own acts and omissions that do not comply with the Data Protection Laws. This duty to indemnify, defend, and hold harmless includes fines that may be imposed by a governing authority and any and all reasonable attorneys' fees and court costs.

15.5 The Parties agree that where Processor processes Personal Data, it functions as a Service Provider and a Processor under the Data Protection Laws.

16. Final Clauses

16.1 By signing this Agreement, Processor certifies that it understands the restrictions herein and will comply with them.

16.2 The obligations contained in this Agreement, including the Exhibits, Attachments, and Appendices, shall not restrict Processor in its rights and/or obligations to: (a) comply with federal, state, or local laws, or to comply with a court order or subpoena to provide information or legal holds, or (b) to comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

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

16.4 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.

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

16.6 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.

16.7 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

.....	Karlsruhe, 2025-09-02
(Place and Date)	(Place and Date)
.....	WIBU-SYSTEMS AG
(Client)	(Processor)
Represented by:	Represented by:
	Sven Maier Signed by: Sven Maier Date: 2026-01-29 11:19:23 CET
(Signature)	(Signature)
.....	Dr. Sven Maier, Data Protection Officer
(Name), (Function)	
(Signature)	
.....	
(Name), (Function)	

Issue date: 2026-02-01

Annex 1: Information about Data Processing

1. Types of Personal Data

Depending on the type of Agreement, different types or categories of data are subject to collection, Processing, and use of data:

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 CmCloudContainers	
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	
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 CmCloudContainers	
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	

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

3. The details of the Processing to be carried out under the Agreement are as follow

Roles of the Parties (check the option that applies)	Client:	☑ Controller	☐ Processor	☐ Sub-Processor
	Processor:	☐ Controller	☑ Processor	☐ Sub-Processor
	If neither Client nor Processor is the Controller, identify the Controller:			
Subject Matter of Processing				
Processing Instructions	Client instructs Processor to Process Personal Data to provide the Services set forth in the Agreement, which include (please provide a general description of the Services provided by Service Provider):			
Duration of Processing	As set forth in the Agreement			
Nature and Purpose of Processing	As set forth in the Agreement			
Types of Personal Data Processed	☐ Abilities/aptitudes	☐ Education records (e.g., transcript)	☐ Iris/retina scan	☐ Professional licenses
	☐ Address	☑ Email address	☐ Keystroke patterns	☐ Purchase/Service history
	☐ Attitudes	☐ Employee ID	☐ Marital status	☐ Religion
	☐ Background checks	☐ Employment history	☐ Medical claim history	☐ Resume
	☐ Bank account number	☐ Eye color	☐ Medical conditions	☐ Signature
	☐ Bank routing number	☐ Facial images	☐ Medical device identifiers	☐ Sleep patterns
	☐ Beneficiary information	☐ Financial records	☐ Medical photo images/X-Rays	☐ Social Insurance Number
	☐ Beneficiary number	☐ Finger or handprint	☐ Medical record number	☐ Social Security number
	☐ Blood pressure	☐ Gender/Gender Identity	☐ Medical test results	☐ State ID
	☐ CCTV footage	☐ Genetic information	☐ Medication	☐ Subscriber number
	☐ Citizenship Status	☐ Govt-issued ID number	☐ Mental health	☐ Survey responses
	☐ Compensation information	☐ Handicapped status	☑ Name	☐ Tax information
	☐ Credit history	☐ Health records	☐ National ID Card Number	☐ Telephone number
	☐ Criminal history	☐ Health status	☐ National origin/race/ethnicity	☐ Union membership or information
	☐ Date of birth	☐ Health symptoms	☐ Partial Social Security number	☐ Vehicle License Plate Number
	☐ Dates of health service	☐ Health treatments	☐ Passport number	☐ Vein patterns
	☐ Diagnosis	☐ Height	☐ Payment card number	☐ Veteran/Military Status
	☐ Disability	☐ Immigration/VISA	☐ Performance Evaluations	☐ Voice patterns
	☐ Disease/disorder	☐ Insurance information	☐ Philosophical beliefs	☐ Voice recordings
	☐ Driver's license number	☐ Insurance policy numbers	☐ Political party	☐ Weight
	☐ Education history information	☐ Intelligence	☐ Preferences, Trends, Predispositions	
	☐ Other:			
Categories of Data Subjects Whose Personal Data Is Processed	☑ Employees	☐ Vendors/Third Parties	☐ Merchant	☐ Website visitors
	☐ Job applicants	☐ Vendor employees	☑ Client employees	☑ Consumers
	☐ Dependents/Beneficiaries	☑ Clients/customers	☑ Application/website users	☐ Client customers
	☐ Former Employees	☐ Potential clients/customers	☐ Minors	
	☐ Other:			

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 Processors, 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 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 workstation, 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 data media is affected 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

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 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							✓

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 Traschuetz, Director Wibu Operating Services (WOPS)
Address	Zimmerstrasse 5, 76137 Karlsruhe, Germany
Phone	+49 721 93172-43
Email	uwe.traschuetz@wibu.com

Data protection Officer of the Processor:

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

Issue date: 2026-02-01