Agreement regarding commissioned processing of personal data
Eplan as Contractor

- The Customer (Contracting Party of EPLAN) and the Contractor (EPLAN GmbH & Co. KG) are hereinafter also, each individually, referred to as a **"Party"**, and collectively, as the **"Parties"** -

This agreement regarding commissioned data processing (the **"Agreement"**) specifies in more detail the Parties' duties under data protection law which result from commissioned processing of personal data in connection with the use of the EPLAN Cloud (hereinafter also the **"Main Contract**") in accordance with Article 28 of Regulation (EU) 2016/679 (**"GDPR"**).

This Agreement applies to the following activities and/or groups of persons, who/which are entrusted to the processing of personal data commissioned by the Customer (Customer's Data) in connection with the main contract:

- To the employees of the Contractor and/or third parties commissioned by the Contractor who come into contact with personal data for which the Customer is a "Controller" by means of the GDPR or
- Regarding the processing of personal data by employees of the Contractor, if the Customer itself is a Processor by means of the GDPR – because it processes personal data commissioned by a third party – instating the Contractor as a subprocessor.

1. Definitions

The definitions in Article 4 GDPR apply to the terms defined in this Agreement, unless they are defined otherwise. A list of the definitions of particular relevance to this Agreement is attached hereto as Appendix to section 1.

2. Contractual components and order of priority

(1) This Agreement, including its appendices, forms a direct and binding part of the Main Contract. In case of doubt, this Agreement takes priority over any provisions of the Main Contract, unless expressly stated otherwise in this Agreement or an appendix.

The duties relating to data protection set out in this Agreement, including its appendices, constitute material contractual duties (principal duties) for the Contractor.

(2) In the event of any gaps or inconsistencies, the following descending order of priority, on the basis of which the contents of the contract will be determined, will apply, it being understood that the appendices to this Agreement rank equally among each other:

- this Agreement
- appendices to this Agreement
- Main Contract, including its appendices

The provisions of the Main Contract will apply to the determination of the priority of the Main Contract and its appendices. If no provision is included there, it will be assumed for the interpretation of this Agreement that the appendices to the Main Contract take priority over the Main Contract.

3. Determination of the subject matter, type and purpose of the commissioned data processing

(1) The Contractor shall process the Customer's data exclusively within the scope of the job and only upon the documented instructions (section 4) by the Customer.

(2) Within the scope of this Agreement, the Customer will be responsible for the compliance with the statutory provisions regarding data protection, in particular, for the lawfulness of the transmission of data to the Contractor, the lawfulness of the data processing and the safeguarding of the rights of data subjects.

(3) The type and purpose of the data processing follows from the Main Contract, in particular, the specification of services (if any). If the Main Contract does not contain any description, or only an insufficient description, regarding the subject matter of the commissioned processing, the Parties have specified the subject matter of the commissioned processing in more detail in appendix to sec. 3.

(4) Unless this results from the Main Contract, the type and purpose of the processing, the type of the personal data, as well as the categories of data subjects, are also specified in more detail in the appendix to sec. 3.

(5) The provisions of this Agreement will apply *mutatis mutandis* if the subject matter of the Contractor's activities is the audit or maintenance of automated procedures or of data processing systems (including by way of administrative access), and if an access to personal data cannot be excluded in that context.

4. Instructions by the Customer

(1) The processing of personal data will be made exclusively within the scope of the arrangements made, unless there exists an exception in accordance with Article 28, section 3a) GDPR. Any information to data subjects or third parties by the Contractor require the prior written consent by the Customer.

(2) Any instructions must be in writing or text form; oral instructions will only be admissible as an exception in urgent cases. In such case, the instructions will subsequently be documented by the Customer in writing or text form without undue delay and will be transmitted to the Contractor.

(3) As a general rule, the Contractor must implement any instructions without any conditions and without undue delay in accordance with the following provisions:

- Before implementing the instruction, the Contractor shall inform the Customer if the Contractor believes that the giving of an instruction, for example regarding the deletion of data of the Customer, will result in the Contractor's no longer being able to provide its products or services owed under the respective Main Contract, or that an access to the services, for example, the log-in to the user accounts, will no longer be possible. If the Customer confirms the instruction, this will be made at the Customer's risk, and the Customer will not be in a

position to invoke any limitation in relation to the Contractor's services caused thereby.

- If the Contractor believes that an instruction violates provisions under data protection law, the Contractor shall notify the Customer thereof without undue delay in writing or text form. In such case, the Contractor may suspend the implementation of the respective instruction until the instruction is confirmed or modified by the Customer.

(4) All communications between the parties shall be conducted exclusively via the email address: Digitale-plattform@eplan.de.

(5) In other respects, any objections, pleas or rights of retention in relation to the Customer's data and their processing are excluded.

(6) The Contractor will use the Customer's data for no other purpose than the purposes for which the Customer has given instructions; in particular, the Contractor may not disclose the Customer's data to third parties, or tolerate an access to them, without a pertinent instruction by the Customer. No copies or duplicates of the Customer's data will be prepared without the knowledge of the Customer. Excluded therefrom are backup copies prepared in the ordinary course of business or the storage of the Customer's data, to the extent that this is required to warrant proper data processing or in relation to the compliance with statutory retention duties.

(7) Any instructions in excess of the scope of services laid down in the Main Contract, which do not serve the purpose of specifying in more detail the existing performance obligations under data protection law, will not be binding for the Contractor within the meaning of section 4 (3) above; rather, they require an express agreement between the Parties to be effective. If the Main Contract provides for a formal change procedure for changes to services and/or modifications of the contract, that procedure must be considered accordingly.

5. Technical and organisational measures

(1) In its sphere of responsibility, the Contractor shall take, for the duration of this Agreement, the measures regarding the security of processing set out in Article 32 GDPR. In so doing, the Contractor shall structure its internal organisation, in consideration of

- the state of technology from time to time,
- the implementation costs,
- the type, scope and the circumstances and purposes of the processing, and
- the varying probability of occurrence and severity of the risk regarding the rights and freedoms of the data subjects,
- such that they meet the special requirements relating to data protection in accordance with the GDPR and warrant the protection of the rights of the data subjects.

(2) The technical and organisational measures to be taken include, in particular:

- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services,
- the pseudonymisation and encryption of personal data,
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident,
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(3) The Contractor has documented the measures. It has taken in an **Appendix to section 5 - Technical and organisational measures by Contractor**.

(4) The measures taken by the Contractor are subject to technical progress and further development. The Contractor may implement alternative adequate measures. In so doing, the security level of the previous measures may not be fallen short of. Any material changes must be documented and be submitted to the Customer for review. In that respect, the technical and organisational measures of Contractor must be reviewed by the Contractor at least once annually upon the Customer's request as to whether the measures taken still adequately reflect them; otherwise, they must be updated.

(5) The Contractor may substantiate the adequacy of the technical and organisational measures, in particular, those to be taken pursuant to Article 32 GDPR, by furnishing evidence of

- the compliance with approved codes of conduct pursuant to Article 40 GDPR; or
- the compliance with an approved certification mechanism pursuant to Article 42 GDPR.

The submission of a certificate by an accredited certification body pursuant to Article 43 GDPR will be sufficient therefor; a copy of such certificate shall then also be attached to the contract as an **Appendix to section 5 - Technical and organisational measures by Contractor**.. The submission of a certification will not limit the Contractor's responsibility for the existence of an adequate protection level or relevant guarantees.

(6) The Customer reserves the right to audit the compliance with the measures referred to in sections 5 (1) to 5 (5) (inclusive) above within the scope of the Customer's audit and monitoring rights (section 13).

6. Rights of data subjects; Support services

(1) The Customer is responsible to safeguard the rights of data subjects in accordance with Chapter 3 of the GDPR. If any such rights are asserted directly as against the Contractor, the Contractor shall forward the request to the Customer without undue delay. This will only apply to the extent that the Contractor is able to allocate the request to the respective data subject. If the Contractor is unable to make such allocation, the Contractor shall notify the Customer of the inability to identify the data subject, and the reasons therefor, in accordance with Article 11, section 2 GDPR.

(2) If requests by data subjects are not forwarded without undue delay, the Contractor will be liable to the Customer for any delays in the processing of requests by data subjects in consideration of the processing periods specified in Article 12, section 3 GDPR, unless the Contractor is not responsible for the delay

(3) The Contractor may only exercise any rights of data subjects, for example, a request for erasure, upon an instruction by the Customer.

(4) The Contractor shall comprehensively assist the Customer in the fulfilment of requests and claims of data subjects in accordance with Chapter 3 of the GDPR and shall provide staff and operating materials as required in that context.

7. Undertaking to observe data secrecy

(1) The Contractor hereby warrants that the Contractor's staff in charge of the processing of the Customer's data:

- will not process any of the Customer's data outside the scope of the Customer's instructions;
- have been instructed about their duties to observe data protection, the confidential treatment of the Customer's data and to maintain confidentiality; and
- have given a personal undertaking regarding data protection, the observance of confidentiality and the duty to maintain secrecy.

The same applies *mutatis mutandis* to any applicable additional confidentiality and/or protective provisions under data protection law (e.g., a statutory duty of professional secrecy). The duty to maintain confidentiality/secrecy must survive the end of the activities of the related employees for the Contractor.

(2) Suitable evidence of the instruction and undertaking of the employees in charge in accordance with section 7 (1) above (e.g., sample undertaking) must be furnished to the Customer upon request.

(3) The Contractor may also comply with its duty under section 7 (1) above by furnishing evidence of the compliance with an approved code of conduct (Article 40 GDPR) or an approved certification mechanism (Article 42 GDPR), provided that it follows therefrom that the employees used for the processing have given an undertaking in accordance with section 7 (1) above.

8. Notification of personal data breaches

(1) The Contractor shall in all cases, and regardless of the attribution of fault (if any), notify the Customer, if the Contractor becomes aware of

- an actual violation of the protection of personal data by the Contractor or any of the Contractor's employees;
- a violation of statutory provisions regarding the protection of personal data; or
- a violation of the provisions of this Agreement

(Each a "**personal data breach**"). A personal data breach must be notified to the Customer without undue delay, and 36 hours after having become aware of it, at the latest.

(2) To the extent that this is possible when becoming aware of a personal data breach, a notification of a personal data breach must include any information which the Customer requires to comply with its duties under Article 33 and Article 34 GDPR, in particular:

- a description of the nature of the personal data breach including, wherepossible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- the name and contract details of the Contractor's data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach;
- a description of the measures taken or proposed to be taken by the Contractor to remedy the personal data breach, to prevent any future incidents and, where appropriate, measures to mitigate its possible adverse effects.

(3) Once the Contractor becomes aware of a personal data breach, the Contractor shall, without undue delay, take the necessary measures to back up the data and to mitigate any adverse effects on the data subjects and the Customer. Should instructions by the Customer be required to do this, the Contractor shall obtain such instructions.

(4) The Contractor shall document any personal data breach in detail, including its effects and the remedial action taken. That documentation must be submitted to the Customer without undue delay.

(5) If the Contractor is not responsible for the personal data breach, section 6 (5) above will apply *mutatis mutandis* to the Contractor's expenses in connection with this section 8.

9. Place of the data processing and third countries

(1) The data will be processed exclusively in

- a Member State of the European Union (EU); or
- a non-EU Member State of the Agreement on the European Economic Area of 2 May 1992 ("EEA Agreement"), once that country has adopted the GDPR in accordance with Article 102, section 1 of the EEA Agreement; or
- a country in relation to which there exists an adequacy decision by the EU Commission (Article 45, section 3 GDPR).

Any data processing outside the aforementioned territories requires the Customer's prior consent.

(2) A consent requires that the special requirements of Articles 44 et seq. GDPR are met on a permanent basis in relation to the processing in question.

10. Subcontractors

(1) The use of additional processors by the Contractor ("**Subcontractors**") will be admissible if all the following requirements are met:

- The use of subcontractors shall be announced by the contractor intime and displayed on the EPLAN homepage at Third-Party (eplan.com) and in the appendix to this section 10. In that respect, the Customer must be provided with appropriate evidence of the following measures upon request.
- The Contractor has carefully selected the Subcontractor and checked the Subcontractor before an instruction as to whether the Subcontractor is able to reliably observe the arrangements made between the Customer and the Contractor, in particular, this Agreement, in professional, technical and organisational terms.
- The Contractor has structured its contractual arrangements with the Subcontractor such that they are at least in line with the provisions regarding data protection in the contractual relationship between the Customer and the Contractor, in particular, this Agreement, and the Subcontractor has, in particular, furnished adequate guarantees under data protection law within the meaning of the GDPR that the Subcontractor will implement adequate technical and organisational measures such that the processing will be made in accordance with the requirements set by the GDPR. To this end, the Contractor may disclose to the Subcontractor the sections of the contractual arrangements made between the Customer and the Contractor, in particular, this Agreement, which are relevant to data protection.
- The Subcontractor has granted to the Customer direct rights to give instructions, monitoring and audit rights in accordance with Article 28(3)(f) GDPR, in conjunction with section 13 of this Agreement ("genuine contract for the benefit of a third party"). Those rights to give instructions, monitoring and audit rights also apply in favour of any customer of the Customer as well as any supervisory authorities which are competent for the Customer, a customer of the Customer, the Contractor or the Subcontractor.
- The Contractor will structure the subcontracting relationship such that the Contractor may assign to the Customer upon request rights under the subcontracting relationship and/or will authorise the Customer to the effect that the Customer may exercise the Contractor's rights under the subcontracting relationship.

(2) The disclosure of the Customer's data to the Subcontractor, as well as the commencement of the processing activities, will not be admissible until all requirements set out in section 10 (1) above are met.

(3) In the daily business, the Customer will contact a Subcontractor only after consultation with the Contractor, the Contractor will coordinate any requests by the Customer with the Subcontractor and will forward relevant feedback or reports.

(4) The Contractor shall inform the Customer via notification function in the EPLAN CLOUD at least 4 weeks in advance of the inclusion of additional Subcontractors. Excepted therefrom are the Contractor's affiliated undertakings, whichmay be used as subcontractors if the Contractor informs the Customer thereof before their first engagement; in that respect, the Customer hereby grants a general authorisation within the meaning of the first sentence of Article 28, section 2 GDPR.

(5) If the Customer does not agree with the use of a Subcontractor, he shall have a special right of termination. The special right of termination must be expressed in text form within a period of 4 weeks after the announcement of the cooperation with the Subcontractor on the EPLAN homepage. If the special right of termination is not exercised within this period, the Customer's consent to the subcontracting shall be deemed to have been provided. In the event that the special right of termination is exercised in due time, the termination shall take effect at the time of the start of the subcontracting.

(6) “Subcontracting relationships” for the purposes of this section 10 do not include any services used by the Contractor from third parties as an ancillary service and as support in performing its job, such as telecommunications services, maintenance and user service, cleaning staff or auditors.

11. Surrender and deletion of data and data carriers

(1) The Customer can export his data himself at any time.

(2) After the end of this Agreement, and at any time before the end of this Agreement upon the Customer’s request, the Contractor shall surrender to the Customer, or a third party named by the Customer, all documents, data carriers, processing and use results, as well as datasets, which came into the Contractor’s possession and which relate to the contractual relationship or were created in connection with the performance of the contract, or shall delete the same upon the express request by the Customer. The surrender shall be in a standard format usual in the industry upon the Customer’s request.

The duty to surrender also covers copies and/or reproductions of data carriers and/or datasets. A right of retention does not exist. The surrender must be made without any pleas or objections. Any transmission costs, as well as any other expenses in connection with the surrender, shall be borne by the Contractor. Section 6 (5) above applies *mutatis mutandis*.

(3) After the surrender of the data in accordance with section 11 (1) above, or if the Customer orders a deletion, any data which may still exist on the Contractor’s data carriers shall be destroyed, or deleted, in accordance with data protection requirements. The final deletion of the data requires the Customer’s agreement. Upon request, the Contractor shall furnish evidence to the Customer of the completion of the deletion by suitable documents and/or a corresponding self-declaration.

If the Contractor is obliged under statutory provisions to retain data or materials which contain Customer’s data, the processing will be limited. The data or materials in question may only be used to comply with the retention duties and will be blocked by the Contractor for any other purpose. Any such materials and personal data shall be kept by the Contractor in a manner which, during the term of their retention, is at least in line with the requirements set out in this Agreement, regardless of the termination of this Agreement or the Main Contract. After the expiry of the corresponding time limits, the related data or materials will be destroyed in the Contractor’s ordinary course of business. The first sentence of this section 11 (2) applies *mutatis mutandis*.

The same applies *mutatis mutandis* if the deletion of the data and materials is not possible at reasonable technical or temporal expense owing to the special type of storage or is only possible at disproportionately high costs.

(4) Any documentation which serves as evidence of the proper data processing in line with the job must be retained by the Contractor after the end of this Agreement in accordance with the respective retention periods. The Contractor may discharge this duty if the Contractor submits the documentation to the Customer upon the end of this Agreement.

(5) The provisions of sections 11 (1) and 11 (2) above apply *mutatis mutandis* to any test and scrap materials. The costs of the destruction shall be borne by the Customer.

12. Additional duties of the Contractor

(1) The Contractor shall provide the details and information regarding the commissioned processing which are required for the records of processing activities to be maintained by the Customer in accordance with Article 30 GDPR. Upon the Customer's request, such provision must be made in an editable standard format usual in the industry.

(2) The Contractor shall advise and assist the Customer in the compliance with the duties under Article 32 GDPR. To this end, the Contractor shall provide the Customer with the documents and evidence for the documentation of the measures pursuant to Article 32 GDPR, and shall, without being asked, provide any updates of those materials which are created in the course of the performance of this Agreement.

(3) The Contractor shall advise and assist the Customer in the performance of, and compliance with, the data protection impact assessment in accordance with Article 35 GDPR.

(4) To the fullest extent permitted by law, the Customer must, without undue delay, be informed of any monitoring actions and measures by a supervisory authority, in particular, in accordance with Article 58 GDPR. This applies also if a competent authority conducts investigations with the Contractor.

(5) In relation to the performance of this Agreement, the Contractor shall regularly review the compliance with and, if applicable, any necessary adaptation of, provisions and measures to perform the job. The Contractor shall inform the Customer without undue delay of any faults and/or irregularities discovered thereby and shall obtain the decision by the Customer.

(6) To the extent required by law, the Contractor shall appoint a data protection officer, who is able to perform his activities without any restrictions in accordance with Article 37 and Article 38 GDPR. The Contractor shall advise the Customer, without being asked, of the contact details of the data protection officer or - if no data protection officer is required to be appointed - another contact for data protection issues authorised to make decisions for the purpose of direct contacting, as well as of any changes.

(7) Should data of the Customer be jeopardised with the Contractor as a result of attachments or seizures, insolvency or composition proceedings or other events or third-party measures, the Contractor shall inform the Customer thereof without undue delay, to the fullest extent permitted by law. The Contractor shall, without undue delay, inform all persons who are responsible in that context that the sovereignty and ownership in relation to the data rests exclusively with the Customer as "controller".

13. Customer's monitoring and audit rights

(1) The Customer may, in consultation with the Contractor, carry out audits, or have them carried out by third parties or auditors subject to a duty of confidentiality in an individual case. In particular, the Customer may satisfy itself of the compliance with this Agreement in the Contractor's business during the Contractor's usual business hours by random inspections.

(2) Upon request, evidence of the existence of corresponding confidentiality agreements must be furnished to the Customer. Professional duties of confidentiality will be sufficient, to the extent that they are punishable by operation of law, for example, lawyers or tax advisors. The Contractor may only reject an auditor if the related person acts for a direct competitor of the Contractor. Any auditors sent to the Customer or a customer of the Customer by supervisory authorities do not require a special confidentiality agreement, and a right of rejection will not exist.

(3) Normally, an audit must be announced at fourteen (14) days' notice. In urgent cases, the Customer may shorten the notice period to 24 hours. An urgent case will exist, in particular, if:

- there exist specific reasons to believe that the Contractor continuously breaches statutory provisions regarding data protection or violates the provisions of this Agreement,
- there exist specific reasons to believe that a duty to notify by the Customer exists under Article 33 GDPR or another statutory provision as a result of a breach of statutory provisions regarding data protection or a violation of the provisions of this Agreement by the Contractor exists, or
- the Customer, or a customer of the Customer, becomes subject to an inspection or audit by a data protection supervisory authority or another supervisory authority, and the subject matter of the inspection or audit also relates to the Contractor.

(4) The Contractor hereby warrants that the Customer and the auditors instructed by the Customer will be able to convince themselves of the compliance with the Contractor's duties under Article 28 and Article 29 GDPR in relation to the contractual commissioned processing of the Customer's data. The Contractor shall provide the Customer with any necessary information and shall, in particular, furnish evidence of the implementation of the technical and organisational measures in accordance with Article 32 GDPR.

(5) The Contractor's support services in the carrying out of audits (e.g., expenses, personnel) will be compensated by the remuneration under the Main Contract in the event of one audit per year, as well as in the event of any audits occasioned by culpable conduct of the Contractor, or audits occasioned by supervisory authorities.

(6) The Customer may exercise the above-mentioned monitoring and audit rights during the term of this Agreement and during a period of three years after the termination of this Agreement.

14. Customer's duties

(1) The Customer will be liable for the compliance with the statutory provisions regarding data protection, in particular, for the lawfulness of the transmission of data to the Contractor and the lawfulness of the data processing.

(2) The Customer shall fully inform the Contractor without undue delay if the Customer establishes errors or irregularities in relation to provisions regarding data protection law in the review of the processing results.

(3) The Customer shall keep public records of processing activities in accordance with Article 30 GDPR. The Contractor's duty to keep its own records of processing activities in accordance with Article 30, section 2 GDPR remains unaffected thereby.

(4) The Customer shall name a competent contact for the data protection issues which arise under this Agreement and shall advise the Contractor of the contact details for direct contacting.

15. Term and termination

(1) This Agreement enters into force upon its signing by both Parties and runs for an indefinite period. This Agreement ends upon the termination of the Main Contract, provided that, if the Main Contract contains post-contractual duties which cover the

processing of the Customer's data, this Agreement will not end before any such duties end. No separate notice of termination will be required.

(2) The Customer may terminate this Agreement, including the Main Contract, for good cause with immediate effect if:

- the Contractor culpably breaches statutory provisions regarding data protection and/or any of the duties under this Agreement and fails to remedy such breach within thirty (30) calendar days despite a reminder; or
- the Contractor culpably breaches statutory provisions regarding data protection and/or any of the duties under this Agreement, and the consequences of such breach result in damage or liability claims of third parties, or a duty of the Customer to pay a fine, in an amount of more than EUR 10,000; or
- the Contractor culpably breaches any of the technical and organisational measures to be taken pursuant to section 5 above, and if this results in breach of the security of the Customer's data.

(3) If this Agreement ends - for any reason whatsoever - each Party may suspend those performances under the respective Main Contract which require the processing of the Customer's data until the Parties agree on the further procedure, for example, the conclusion of a follow-up main contract or the termination of the Main Contract. Any performances in relation to which no Customer's data are processed shall be continued to be rendered. Any claims based on the discontinuance of the performance, in particular, claims for damages or claims to the reduction of current remuneration, will be excluded.

16. General provisions

(1) In the processing of the Customer's data and in the interpretation of the requirements of the GDPR, as well as of the provisions of this Agreement, the Parties shall reasonably consider the recommendations of Article 29 Data Protection Working Party or its successor organisation (European Data Protection Board). In case of doubt, the recommendations will govern the average type and quality of the performances owed by the Contractor.

(2) The Parties agree to adapt and/or amend this Agreement, including its appendices, to the extent that this is necessary as a result of modifications, adaptations and/or amendments of statutory provisions, in particular, the GDPR and/or the national data protection provisions applicable from time to time. Unless agreed otherwise herein, any modifications will always be made by mutual agreement. If the Main Contract provides for a formal change procedure, either Party may demand that such procedure also be applied to any modifications of this Agreement.

(3) The Parties shall inform one another if they believe that a change to statutory provisions regarding data protection will affect the Contractor's duties to the Customer under this Agreement or the respective Main Contract and will require a modification of this Agreement or its appendices. The Parties shall bring about a mutually acceptable solution, while also considering the impact of any such measure on the agreed remuneration.In other respects, the provisions of the Main Contract apply.

List of appendices:

- Appendix to sec. 1 – definitions
- Appendix to sec. 3 – determination of the subject matter, type and purpose of the commissioned data processing
- Appendix to sec. 5 technical and organisational measures
- Appendix to sec 10 – Subcontractors

Appendix to sec. 1 - Definitions

"**Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. In connection with this Agreement, theContractor is the processor; the Customer may, however, also be the processor of a third-party customer.

"**Employee**" means

- salaried employees, including temporary workers in the relation to the hirer,
- apprentices and trainees, including interns,
- participants in state-regulated benefits to promote the participation in employment,as well as in assessments of occupational ability or job testing (rehabilitants),
- employees in state-approved workplaces for disabled persons,
- persons working in a voluntary service regulated by law,
- persons who are considered to be employees owing to their economic dependence;these also include home workers and persons treated as such,
- civil servants, judges, soldiers and persons doing community service, regardless ofthe governmental body which employs them.

Applicants for an employment and persons whose employment has ended are alsoconsidered to be employees.

"**Special categories of personal data**" means personal data within the meaning of Article9 GDPR, i.e., personal data revealing racial or ethnic origin, political opinions, religious orphilosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

"**Third party**" means a natural or legal person, public authority, agency or body other thanthe data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

"**Consent**" of the data subject means any freely given, specific, informed and unambiguousindication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

"**Personal data**" means any information relating to an identified or identifiable natural person ("**data subject**"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processingof personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may beprovided for by Union or Member State law. In connection with this

Agreement the Customer is the Controller. The Customer may, however, also be a Processor of a third party Controller

"**Processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Affiliated undertakings**" means legally independent business enterprises which a) holdthe majority of the shares or voting rights in another business enterprise (majority shareholding) and business enterprises subject to any such majority shareholding, or b) areable to exert a direct or indirect controlling influence on another business enterprise (controlrelationship) and business enterprises subject to such control relationship, or c) are subject toa common management or have another dependent relation among each other (group relationship).

"**Instruction**" means an instruction by the Customer to the Contractor in respect of a specific treatment in accordance with data protection (e.g., anonymisation, blocking, deletion, surrender). Instructions are determined in the Main Contract and may be supplemented by the Customer thereafter by individual instructions under this Agreementwhich put the Main Contract in more concrete terms.

Appendix to sec. 3 - Determination of the subject matter, type and purpose of the commissioned data processing

1. Subject matter, type and purpose of data processing

2. EPLAN offers the Customer the use of the EPLAN Cloud, on which the Customer's employees after creating an account and the associated storage of the account data (as described in the EPLAN Cloud Terms of Use) can collaborate with internal and external colleaguesin the engineering process and exchange data. Within the EPLAN Cloud, the Customer has its own encapsulated unit, called organization, to which it can invite users via e-mail address and authorize them to access data and applications.

3. Type of personal data

The following types/categories of data are the subject matter of the

☒ processing:Person master data
☒ Communications data (e.g., phone, email)

4. Categories of data subjects

The following categories of data subjects are the subject matter of the processing:

☒ Clients
☒ Employees
☒ Suppliers

5. Place of processing

Microsoft Azure data centers within the EU.

Appendix to sec. 5 - Technical and organisational measures

Pursuant to Article 32 of the EU General Data Protection Regulation (GDPR), all bodies which collect, process and use personal data are obliged to implement “technical and organisational measures” (hereinafter “TOM”) to warrant that the requirements of the GDPR are met.

Rittal Software Systems GmbH & Co. KG (hereinafter “RSS”) is a member of the Friedhelm Loh Group (hereinafter “FLG”), consisting of EPLAN GmbH & Co. KG and CIDEON Software and Services GmbH & Co. KG and has defined, for itself and its affiliated enterprises, the following TOM for internal and external application.

The measures laid down herein are not disclosed in detail, particularly for security reasons, i.e. for the minimisation of security risks regarding access to company data and respective protection of trade and business secrets; rather, they merely serve as a general standard in order to meet the aforementioned requirements.

The structure of these TOM follows the requirements of Article 32 GDPR and the related annex.

1. Warranting confidentiality (Article 32, section 1b GDPR)

1.1. Entry control

RSS has taken measures regarding entry control to prevent that unauthorised persons have (physical) access to data processing systems which process personal data. This includes:

- Building security
  - Fences, doors/gates
  - Reception staff
  - Video surveillance
  - Visitor’s badges and visitors list
  - Security services outside business hours
- Room protection
  - Safety locks
  - Chip car readers
  - Code locks
  - Safety glazing
  - Alarm systems

The server rooms of RSS are split into several security areas with different access authorisations. Outside business hours, they are monitored by a security service.

The buildings of RSS may (outside customary business hours) only be accessed with coded employee identity cards with the relevant authorisation, or with keys which were handed over to the respective authorised employees, as well as by those instructed persons of RSS who have a corresponding written authorisation and identity cards or keys, respectively. During customary business hours visitors will be registered and marked as a visitor by the reception staff, who will also by issue respective visitor badges. Outside customary office hours visitors will be supervised by the welcoming employee.

Server rooms and/or engineering rooms are secured by conventional locking systems and may only be accessed by defined responsible employees of RSS-IT.

As regards buildings or rooms of RSS equipped with an alarm system, only those employees of the respective location who necessarily require such access in order to fulfil their business duties will be given an activation or deactivation code.

Within the individual security areas, depending on the security level, measures such as safety locks or additional electronic card readers have been implemented.

All employees must wear their employee identity card on the body such that it can be seen. The employee identity cards must at least show the employee's name and the employee's organisational assignment within RSS.

Ideally, visitors will register at reception in advance; in any event, visitors may only access buildings of RSS after a registration at reception. Visitors must prove their identity by a photo ID, wear their visitor's badge on the body such that it can be seen and may only move around the building accompanied by employees of RSS.

1.2. System access control

RSS has taken measures regarding access control to prevent that unauthorised persons gain access to the data processing systems (hereinafter "Data Processing Systems"). This includes:

- Securing the access to computers/systems (authentication)
  - User ID with password and password directives according to the currently valid password guideline (including special characters, minimum length)
  - Biometrical user identification
  - Firewall
  - Certificate-based access authorisation
  - Encryption of accesses to the network via VPN
  - Automatic blocking (e.g., password or automatic pausing, time lapse)
  - Encryption of data carriers (e.g., BitLocker)

Client systems in the network of RSS may only be accessed by a password-based network authentication. The applicable password directive governs, inter alia, the

password procedure (minimum length, complexity, password history). Password uses are recorded in the log files of the individual systems (if applicable).

A direct external access (i.e., from outside the RSS network) is only possible through secured and encrypted connections and security tokens, as well as by a computer/laptop (or similar hardware) provided by RSS (hereinafter “RSS Computer”); other adequate access options are possible in exceptional cases with the written consent by RSS.

Firewalls and proxy servers are used for a safe access to third-party systems. If an encryption of the transmission path to the client is required (VPN), such encryption will be made after joint consultation in accordance with the state of technology and on the basis of the execution of corresponding confidentiality and data processing agreements.

1.3. Data access control

a) General measures

RSS has taken measures which ensure that the users who are authorised to use Data Processing Systems can only access content for which they are authorised. In addition, the intention is to warrant that any personal data can neither be modified nor copied or deleted without authorisation in connection with their processing, storage and use in Data Processing Systems of RSS. This includes:

- Authorisation concept
- User ID and password
- Secured interfaces (USB, Firewire, network etc.)
- Data media administration
- Certificate-based access authorisation
- Integration into employee onboarding/offboarding processes and regular checks whether rights are still needed

The basis is an RSS authorisation concept with a corresponding definition of user profiles and roles with regard to all RSS IT systems. Generally, authorisations will be granted in accordance with the “least privileged” principle, i.e., users will only be granted the authorisations in the respective RSS IT system which they require to perform their duties. Access to an RSS IT system will always be through a user account with a user ID and password.

b) Network

The registration is made through a personal registration account. The dedicated password must comply with the currently valid password directive. IT system administrators use a dedicated personalised administrator account for the work on server systems. Differentiated access rights are defined for files. Accesses in the network are recorded through a log entry on the related servers.

c) RSS systems

RSS operates its own local systems in addition to those provided by FLG. Separate accounts are sometimes required for the RSS systems, provided that these systems do not reference the central (Azure) Active Directory accounts (SSO). Depending on the system, the statements made in section 3 above apply. Interfaces between RSS IT systems use a system account and are password-protected. In addition, the data exchange through the external interfaces will be encrypted (SSL or IPSec, respectively). Furthermore, web service interfaces will be secured by separate FLG or RSS certificates, with the certificate being checked upon each transaction (access).

d) FLG systems

FLG accounts are required for the FLG systems used by RSS. RSS employees can only access the FLG systems through those FLG accounts. Depending on the system, the statements made in section 3 above apply. Interfaces between RSS and FLG IT systems use a system account and are password-protected. In addition, the data exchange through the external interfaces will be encrypted (SSL or IPSec, respectively). Furthermore, web service interfaces will be secured by separate FLG or RSS certificates, with the certificate being checked upon each transaction (access).

e) Client systems

There exist individual applications in client support and consultancy where RSS or its affiliated enterprises require access to client systems by its employees. Of course, the necessary documents (such as confidentiality agreements) will be executed in advance in such cases. Any such access requires an authentication on the part of the RSS employees, as well as special software, hardware, certificates and tokens. In addition, RSS must ensure that only the named employees can access the client-specific access data and devices.

1.4. Destruction of data

The measures regarding the deletion of data have been included in the deletion concept of RSS (cf. section 7). Rules for the deletion of data have been defined therein. In addition, it is warranted that extraordinary deletion jobs (e.g., deletion requests by a data subject) can be implemented without undue delay.

Confidential data on paper or electronic data media such as hard disks or backup tapes will be destroyed in a professional manner by specialist firms in accordance with the current state of technology. In addition, all data media will be overwritten with random values several times in accordance with a safe procedure before a disclosure.

The deletion concept provides for measures regarding the logging of the data deletion and the handling of special situations (e.g., deletion fails). The confirmation of the deletion process can be transmitted to a customer of RSS in electronic form upon request.

A destruction (deletion) of data in public cloud systems (Office365, Azure) is agreed in the hosting contract, so that the RSS IT system administrators can commission and monitor such data deletion.

1.5. Principle of separation

RSS has taken measures to ensure that personal data used for different purposes, or for different data controllers or customers, are processed and used separately ("multi-client capability").

- Separation of productive and test systems
- Separate file structures (commissioned data processing)
- Separate tables within databases
- Separate databases

All RSS employees have been instructed and trained to collect, process or use personal data only in connection with the provision of the service and in compliance with the intended purpose. Personal data of customers (e.g., clients) will only be used to perform the contract. Personal data of customers (e.g. clients) are used only within the framework of the respective main-contract, for its fulfillment.

The principle of functional separation has been introduced in all key areas. Thereby, all specialist departments involved in the data processing are separated in organisational, functional and spatial terms.

In the RSS IT systems, personal data of the clients or employees are administered through separate meta data or datasets (logical separation). In addition, there exists a separation of test systems and productive systems. The test systems do not contain any "real" personal data and are only created for test purposes with

fictitious contents. That separation also relates to the necessary databases of the IT systems. Through the RSS authorisation concept, the personal data in the respective IT systems are also separated according to the organisational allocation.

In particular, general encryption procedures in accordance with the current state of technology must be considered.

In addition, there also exists a functional separation for sensitive systems into development, test and productive systems, each with separate databases.

1.6. Transmission control

By its TOM, RSS ensures that personal data cannot be read, copied, modified or deleted during the electronic transmission, or during the transport or storage on data media, and that any such access and the transmission of such data can be documented within the RSS IT systems. This includes:

- Protection during the electronic transfer
  - Encryption
  - VPN
  - Firewall
  - Fax logs
- Protection during the transport
  - Sealed containers
  - Encryption
- Protection during the transmission
  - Procedural directory
  - Logs

1.7. Disclosure of data to third parties

While personal data from RSS IT systems will, as a general rule, not be disclosed, a disclosure will be possible if a disclosure to affiliated enterprises, clients, partners or suppliers is admissible under an applicable legal or contractual provision. Depending on the contract with the third party, different data will be affected. In each case, a disclosure of data must be protected by the execution of non-disclosure agreements (hereinafter “NDA”) and agreements regarding commissioned data processing (hereinafter “CDP agreement”) with the respective third party.

Any disclosure will always be for a specific purpose and will be made through connections secured by current encryption mechanisms (SSL or IPSec). Details are set out in internal directives; the RSS employees will regularly be informed of the handling of personal data.

2. Integrity (Article 32, section 1b GDPR)

RSS has taken measures regarding input control which ensure that it can be checked subsequently whether, and by whom, personal data have been entered, modified or deleted.

In most RSS IT-systems, the entry or modification of personal data will be logged by the system itself. In the case of IT systems without automatic logging of the data collector, the collector will be logged. In the case of RSS IT systems with automatic logging of the data collection, the user identification will be made through the user account.

3. Pseudonymisation and encryption (Article 32, section 1, in conjunction with Article 4, section 5 GDPR)

3.1. Filing of client data within the RSS IT systems

Client data are stored and administered in various IT systems of RSS.

Client data may only be used and processed in accordance with the requirements set out herein. RSS does not operate any interfaces between its IT systems and the IT systems of clients to exchange personal data. If personal data are exchanged with clients, this must be done by email or CryptShare (encryption program/add-on). In either case, the data will be transmitted in encrypted form.

4. Availability (Article 32, section 1b GDPR)

4.1. Availability control

To protect data against loss or accidental destruction, various types of protection programs (virus scanners, firewalls, spam filters etc.) are used both on the RSS computers of the RSS employees and on the servers in the server rooms of RSS or FLG, respectively.

In addition, safety measures (uninterruptible power supply, RAID, monitoring, fire protection, air conditioning, backups) have been implemented to warrant the availability of the data and to protect them against loss or destruction.

Some central RSS applications (CRM, DMS, EPLAN Cloud) are hosted with service providers. The service providers have been contractually obliged by means of commissioned data processing agreements to comply with the statutory requirements regarding data protection, in particular, the GDPR.

The respective computer centres of the service providers comply with the availability requirements of Tier III and the availability checks required under the GDPR. The measures regarding availability control must be checked and agreed

within the scope of the hosting contract (commissioned data processing contract).

4.2. Job control

RSS ensures by various technical-organisational measures that personal data processed by means of commissioned data processing will be processed in accordance with the principal's instructions. This includes:

- Definition of powers to give instructions
- E.g., furnishing of evidence of certifications, on-site checks or other adequate guarantees (Article 28 GDPR)
- Agreement in accordance with the standards under Article 28 GDPR or other appropriate legal instruments (e.g., EU standard contractual clauses)
- Random checks
- Concession of monitoring rights

The data received, or collected, for processing will be processed in accordance with the statutory provisions exclusively within the scope of the job or the instructions by the respective customer. Any commissioned data processors will always be obliged in writing under relevant agreements (e.g., commissioned data processing contract in accordance with Article 28 GDPR, EU standard contractual clauses or other appropriate measures).

5. Resilience of the systems (Article 32, section 1b GDPR)

As regards the resilience of the systems, RSS has taken, in particular, the following measures:

- The storage capacity is more than sufficient and can also be extended on short notice
- Systems and services have been, and will be, procured for sustainable use and meet the future requirements
- The bandwidth has been procured for sustainable use and also meets future requirements

6. Data restoration (Article 32, section 1c GDPR)

- Existence and updating of a "data restoration concept" for the ISS IT systems
- Backup-restore-concept for the restoration data lost by reason of e.g. software error, human failure or defect of hardware
- Data backup procedures will be monitored
- Redundant data storage
- Redundant IT infrastructure

- Productive IT-systems have hot- or warm standby systems (partly in separated computer centres depending on the significance of the operated Application), to ensure the availability of the respective applications in case of hardware defects
- The availability concept of the IT-systems will periodically be tested for functionality

7. Testing, assessing and evaluating (Article 32, section 1d GDPR)

The following organisational measures of RSS ensure that the requirements of the GDPR in relation to the protection of personal data are continuously audited, assessed and evaluated:

- Authorisation concepts, directives and work instructions regarding the handling of personal data (e.g., data protection concept) are regularly audited, assessed and evaluated
- The data restoration concept for the RSS IT systems is regularly audited, assessed and evaluated
- Regular further training of the data protection officer
- Regular audit of the technical-organisational measures by the data protection commissioner
- Continuous monitoring of the commissioned data processors, in particular, an analysis of the reporting, applicable Service Levels, as well as an evaluation of necessary changes or specific improvement measures
- The employees of RSS undertake obligation to comply with the requirements under data protection law laid down in Article 5, section 1 GDPR as well as other obligations deriving from particular mandatory local and applicable legal statutes. Those undertakings will be documented in writing; besides all employees undertake obligation to maintain confidentiality
- Continuous instruction of the RSS employees by the data protection officer, or the technical supervisors in accordance with the instructions by the data protection officer, regarding the confidentiality of personal data
- Role and function descriptions for the RSS employees regarding the definition of the responsibilities for specific personal data are reviewed and adapted
- Auditing of RSS by an external institution on a regular basis regarding the lawful implementation of data protection within the enterprise
- In the event of commissioned data processing, audit rights will be exercised with the commissioned data processors

The information security management documents named hereinafter are subject to a regular (at least annual) audit. These documents are inter alia

- information security directive
- security directive – information and data
- security directive - operation and support
- security directive - systems (platform security)
- security directive - networks

Appendix to sec. 10 Subcontractors

The following Subcontractors act with the Customer's consent:

	Name	Contact	Location for contractual relationship of Subcontractors
1.	Microsoft Deutschland GmbH	https://azure.microsoft.com/de-de/support/legal/	Germany (EU)
2.	Twilio Germany GmbH	https://www.twilio.com/legal/tos	Germany (EU)
3.	Hubspot Inc.	https://legal.hubspot.com/legal-stuff	Cambridge (USA)
4.	Google Ireland Ltd.	https://policies.google.com/privacy?hl=de	Ireland (EU)
5.	Adobe Systems Software Ireland Ltd.	https://www.adobe.com/de/legal.html	Ireland (EU)

As a matter of principle, the personal data that EPLAN collects when the Customer uses the EPLAN Cloud is stored and processed on servers within the EU economic area in compliance with the GDPR.

The aforementioned Subcontractors perform the following partial services:

	Description of partial service
reg. 1.	Cloud-Hosting-Service, Data storage (user database, uploaded files)
reg. 2.	E-mail sender of the automated technical mails in the registration process (E-mail address, Surname)
reg. 3.	Analysis tool to optimize the user experience (Origin of the user - previous page - link to the reference)
reg. 4.	Analysis tool to optimize the user experience (browser information: Language, resolution, plug ins installed, type, time zone, duration, previous page).
reg. 5.	Content-Management-System, Hosting the website eplan.com (Name, Email-address, position)