

Schedule to the Main Agreement

Agreement on the Processing of Personal Data in Connection with the Provision of SERVICES (hereinafter: “Data Processing Agreement”)

The contracting parties are ALLPLAN Deutschland GmbH or, if specified in the Main Agreement, an affiliate of ALLPLAN Deutschland GmbH (hereinafter: “ALLPLAN”), and the customer named in the Main Agreement (hereinafter: “the Customer”), (each individually referred to as a “PARTY” and collectively as the “PARTIES”).

Preamble

This AV Agreement governs the rights and obligations of the PARTIES to the extent that, within the scope of the provision of services pursuant to the Terms of Use and License or other written or electronic agreements between ALLPLAN and the Customer, or each individual user (hereinafter: “MAIN AGREEMENT”) regarding the use of web platforms, the provision of cloud services for SaaS products, the provision of support services (via telephone, email, and remote maintenance), or the use of online services (hereinafter: “SERVICES”) results in the processing of personal data by ALLPLAN on behalf of the Customer or an individual user within the meaning of applicable data protection law.

This DPA is an integral part of the MAIN AGREEMENT concluded between the PARTIES. ALLPLAN assumes the obligations described in this DPA toward all customers who enter into a MAIN AGREEMENT with ALLPLAN for the provision of any of the SERVICES listed in **Annex AV1** to this DPA.

This AV Agreement supplements all existing Main Agreements between the Parties and fully replaces all previously concluded AV Agreements.

Updates

If a customer renews or purchases a SERVICE, ALLPLAN may provide the customer with updated provisions of this AV Agreement in writing. Unless the customer objects in writing within four weeks of receiving the notice, the notified provisions of this AV Agreement shall be deemed agreed upon as of the notified date. If the customer objects, the previous General Terms and Conditions shall remain in effect, provided that it is economically reasonable for ALLPLAN to continue them in accordance with applicable legal requirements. We make the current version of these General Terms and Conditions available for download to our customers and users on the ALLPLAN homepage ([Legal Overview - ALLPLAN Deutschland GmbH](#))

Electronic Notifications

ALLPLAN may provide the customer with information and notices regarding SERVICES via email or through the respective SERVICE itself. A notice is deemed to have been given on the date it was made available by ALLPLAN.

Previous Versions of the Terms of Service

The provisions of this AV Agreement apply to the SERVICES currently available. Customers may request previous versions of the AV Agreement from ALLPLAN.

For the purposes of this Terms of Service Agreement, the terms “**supervisory authority**,” “**data processor**,” “**data subject**,” “**third country**,” “**personal data**,” “**processing**,” “**Data Controller**,” and “**Personal Data Breach**” have the meanings assigned to them in Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data, on the free movement of such data, and on the repeal of Directive 95/46/EC (General Data Protection Regulation – “GDPR”) have.

1. Purpose and Duration of Processing

- 1.1 ALLPLAN provides the SERVICES agreed upon in the respective MAIN AGREEMENT to the Customer. To the extent that ALLPLAN receives personal data for processing on behalf of the Customer and/or collects or otherwise processes such data on behalf of the Customer, the Customer shall be deemed the data controller and ALLPLAN the data processor within the meaning of the GDPR. This Data Processing Agreement governs the relevant rights and obligations of the PARTIES.
- 1.2 As an integral part of the MAIN AGREEMENT, this Data Processing Agreement enters into force upon the conclusion of the respective MAIN AGREEMENT and terminates upon its termination. The right of each PARTY to terminate this Data Processing Agreement for good cause remains unaffected. Good cause entitling ALLPLAN to terminate this DPA extraordinarily exists, in particular, if there is a current or future regulatory provision or obligation that subjects ALLPLAN to a regulation or requirement that is not generally applicable, makes it difficult for ALLPLAN to continue providing the SERVICE without modification, and/or leads ALLPLAN to believe that this Service Agreement or the SERVICE may conflict with such a requirement or obligation.
- 1.3 If, following the termination of this Service Agreement, the processing of personal data by ALLPLAN is necessary or required by law to fulfill the MAIN AGREEMENT—for example, with regard to the disclosure of personal data to the Customer—this Service Agreement shall remain in effect until the Main Agreement has been fully fulfilled.

2. Nature and Purpose of the Processing, Categories of Personal Data, and Categories of Data Subjects

- 2.1 ALLPLAN processes personal data exclusively on behalf of and in accordance with the client's instructions, and only to the extent necessary to provide the SERVICES under the MAIN AGREEMENT. The details of the processing—in particular, the nature and purpose of the processing to be performed by ALLPLAN on behalf of the client—are set forth in the MAIN AGREEMENT and its annexes, as well as in Annex AV2 of this AV Agreement.
- 2.2 The Contractor reserves the right to anonymize or aggregate the personal data using state-of-the-art methods so that it is no longer possible to identify individual data subjects—even for the Contractor itself or for third parties—with a reasonable amount of effort, and to use such data in this form for the purposes of needs-based design, further development, and optimization, as well as for the provision of the service agreed upon in accordance with the Main Contract. The parties agree that personal data that has been anonymized or aggregated in accordance with the above provisions shall no longer be considered personal data within the meaning of this Agreement.
- 2.3 The type of personal data processed by ALLPLAN under this AV Agreement on behalf of the Customer pursuant to Art. 28(3) of the GDPR, and the categories of data and data subjects, are set forth in **Annex AV2** to this AV Agreement.

3. Obligations of the Customer

- 3.1 The Customer is solely responsible for compliance with the statutory provisions of the GDPR and applicable national data protection laws applicable to the Customer, as well as, in particular, for assessing the lawfulness

of the commissioned processing and for safeguarding the rights of data subjects pursuant to Articles 12 through 22 of the GDPR.

- 3.2 The Customer shall issue instructions regarding the processing of personal data in writing or in a documented electronic format. In urgent cases, instructions may also be given verbally; verbal instructions must be confirmed by the Customer immediately in writing or in a documented electronic format. Instructions that result in a material change to the nature or scope of the contractually agreed-upon processing shall be deemed requests for modification and may require an adjustment to the compensation and terms of service agreed upon between the PARTIES.

4. Obligations of ALLPLAN

4.1 Compliance with Applicable Data Protection Laws

- (a) ALLPLAN undertakes to comply with the applicable provisions of the GDPR as well as applicable national data protection laws.
- (b) ALLPLAN confirms that a Data Protection Officer has been appointed. The current contact information for the Data Protection Officer can be found in the privacy policy on ALLPLAN's website (<https://www.allplan.com/de/datenschutz/>).

4.2 Processing on Behalf of the Customer

- (a) ALLPLAN processes personal data exclusively in accordance with the provisions of this Data Processing Agreement and—including with respect to the transfer of personal data to a third country or an international organization—in accordance with the Customer's documented instructions, unless ALLPLAN is otherwise obligated by the law of the European Union or the Member States to which ALLPLAN is subject. In such a case, ALLPLAN shall notify the Customer of these legal requirements prior to processing, unless the applicable law prohibits such notification due to an important public interest.
- (b) The MAIN AGREEMENT and this AV Agreement shall be understood as instructions. Within the framework of the product-specific parameters, the Customer determines the nature and scope of the processing through the manner in which the respective SERVICE is used and by selecting the available options, e.g., regarding the scope and nature of the data to be processed.
- (c) ALLPLAN shall immediately inform the Customer if ALLPLAN believes that an instruction violates the provisions of the GDPR or applicable national data protection laws. ALLPLAN is entitled to suspend the execution of the relevant instruction until it is confirmed or amended by the Customer. The PARTIES agree that responsibility for the processing of personal data in accordance with the instructions lies solely with the Customer. ALLPLAN is not obligated to review the legality of the Customer's instructions in terms of content; responsibility for the legality of the instructions lies solely with the Customer.

4.3 Data Security and Confidentiality

- (a) ALLPLAN shall implement appropriate technical and organizational measures to ensure that processing complies with the requirements of applicable data protection laws and that the rights of data subjects are protected. These measures must ensure a level of data security that is appropriate to the risks to the rights and freedoms of data subjects. In particular, ALLPLAN must structure its internal organization in such a way as to ensure compliance with the specific requirements for the protection

of personal data and to protect personal data against accidental or unlawful destruction or alteration, loss, and unauthorized disclosure or access.

- (b) The technical and organizational measures to be taken by ALLPLAN for the respective SERVICES include, at a minimum, the measures described in Annex AV3 of this AV Agreement. ALLPLAN will regularly review, assess, and evaluate the effectiveness of these technical and organizational measures, at least once a year. ALLPLAN will immediately implement any adjustments necessary to maintain data security.
- (c) Notwithstanding Sections 4.3 (a) and (b), ALLPLAN may, as part of the regular review, assessment, and evaluation of the data protection and security concept, adjust the technical and organizational measures set forth in Annex AV3 of this AV Agreement at any time. However, this is subject to the condition that the level of protection provided by the amended measures is not lower than the level in effect at the time this AV Agreement entered into force. In any case, the level of protection required under the provisions of the GDPR must be maintained. ALLPLAN will promptly inform the Customer of any material adjustments to its technical and organizational measures.
- (d) ALLPLAN undertakes to maintain confidentiality when processing personal data. This obligation shall continue even after the termination of this Data Processing Agreement.
- (e) ALLPLAN guarantees the reliability and appropriate supervision of all persons involved in the processing of personal data and ensures in all cases that access to personal data is strictly limited to those persons who need to know such personal data in order to provide the SERVICES to the Customer. ALLPLAN further ensures that only those individuals who have previously been bound by legal requirements regarding confidentiality and compliance with data protection regulations may access the personal data.

4.4 Rights of Data Subjects

- (a) ALLPLAN will immediately inform the Customer if a data subject contacts ALLPLAN directly to exercise their rights and will forward the data subject's request to the Customer.
- (b) The responsibility for responding to requests from data subjects rests solely with the customer.
- (c) However, given the nature of the processing, ALLPLAN will, to the extent possible, support the customer with appropriate technical and organizational measures to fulfill its obligation to respond to requests to exercise the data subject's rights set forth in Chapter III of the GDPR, to the extent that such support is reasonably necessary, technically feasible, and proportionate. The Customer shall reimburse ALLPLAN for the reasonable expenses incurred by ALLPLAN in providing the respective support services. Separate reimbursement may only be claimed if the Customer requested the relevant service with knowledge of the specific costs involved.

4.5 Support for the Customer

- (a) Taking into account the nature of the processing and the information available, ALLPLAN will assist the Customer in complying with the obligations set forth in Articles 32 through 36 of the GDPR—in particular with regard to data protection impact assessments and prior consultations with the supervisory authority—to the extent that is appropriate and necessary and within a reasonable timeframe, to the extent required by applicable data protection law. The Customer shall provide ALLPLAN with

appropriate support in this regard and make the necessary information available in a timely manner. Costs incurred by ALLPLAN as a result of these support measures shall be reimbursed by the Customer to a reasonable extent, unless they arise from a breach of ALLPLAN's obligations for which ALLPLAN is responsible. Separate compensation may only be claimed if the Customer requested the relevant service with knowledge of the specific cost implications.

- (b) ALLPLAN shall inform the customer after a reasonable review and without delay after ALLPLAN has confirmed a breach of personal data protection or has become aware of it, and shall provide the customer with the relevant information reasonably available at that time in accordance with Article 33(3) of the GDPR. To the extent that this information is not yet complete at that time, it may be supplemented in stages or provided subsequently as soon as further information becomes available or is confirmed following a reasonable investigation. ALLPLAN is not obligated to provide information that is not yet reasonably available or has not yet been confirmed prior to the completion of a reasonable investigation.
- (c) ALLPLAN shall immediately inform the customer of any inspections or measures taken by supervisory authorities or other third parties, to the extent that these relate to the processing under this Data Processing Agreement and ALLPLAN is not required by an official order or by law to withhold such information. To the extent that ALLPLAN is required to inform the Customer in accordance with the foregoing, ALLPLAN may not contact a supervisory authority or a third party in connection with the processing of personal data without the Customer's prior consent.
- (d) ALLPLAN shall ensure that all processing activities carried out on behalf of the Customer are documented in accordance with the requirements of Article 30(2) of the GDPR.

4.6 Deletion and Return of Personal Data

Upon termination of this Data Processing Agreement or at the Customer's instruction, ALLPLAN shall, at the Customer's option, delete or destroy all personal data, including all existing copies, and/or return all personal data to the Customer and delete the existing copies, unless there is an obligation under Union law or the law of the Member States to retain the personal data. If additional costs arise due to deviating requirements regarding the return or deletion of the data, these costs shall be borne by the Customer. Separate compensation may only be claimed if the Customer requested the corresponding service with knowledge of the specific cost implications.

The customer must exercise the choice between return and deletion within 30 calendar days of the termination of this General Terms and Conditions Agreement or upon ALLPLAN's receipt of the instruction; after this period has expired, ALLPLAN is entitled, at its discretion, to delete or destroy the personal data or to return it to the customer and subsequently delete any existing copies. ALLPLAN is entitled to retain copies of personal data to the extent and for as long as this is necessary to fulfill legal or regulatory obligations, for data backups, for security reasons, for verification, audit, dispute resolution, or evidentiary purposes, or for archiving. The retained copies will be deleted as soon as the respective retention purpose no longer applies, provided there is no statutory retention obligation. The data will be returned in a standard market format determined by ALLPLAN; any additional support, migration, or conversion services will be provided only for a separate fee.

4.7 Verification of Compliance with This AV Agreement and Audits by the Customer

- (a) ALLPLAN will provide the customer with all information necessary to demonstrate compliance with ALLPLAN's obligations under this AV Agreement.
- (b) The Customer is entitled to verify, to a reasonable extent, ALLPLAN's compliance with the provisions of this AV Agreement, either on its own or through independent third parties commissioned by the Customer and bound by confidentiality obligations. The Customer shall reimburse ALLPLAN for the reasonable expenses incurred by ALLPLAN in connection with an audit. Separate reimbursement may only be claimed if the Customer requested the relevant service with knowledge of the specific cost implications.
- (c) The Customer shall conduct audits only to the extent necessary. To the extent that ALLPLAN provides evidence of the correct implementation of the agreed-upon data protection obligations as described in Section 4.3(b) of this AV Agreement, an audit shall be limited to random sampling. If an audit at ALLPLAN is necessary in an individual case, it must be conducted without causing avoidable disruptions to ALLPLAN's business operations. Unless otherwise indicated for urgent reasons to be documented by the customer, audits shall take place only after reasonable advance notice and during ALLPLAN's business hours, and no more frequently than once every twelve months.
- (d) If, in the course of an inspection, there is a possibility of accessing ALLPLAN's confidential information, ALLPLAN is entitled to require the customer to enter into a confidentiality agreement. Furthermore, ALLPLAN is entitled, at its sole discretion and taking into account the Customer's legal obligations, to withhold information if such information is confidential with respect to ALLPLAN's business activities or if its disclosure would cause ALLPLAN to violate statutory or contractual provisions.

5. Subcontractors

- 5.1 ALLPLAN may engage additional data processors (hereinafter: "SUBCONTRACTORS") to provide the SERVICES. A SUBCONTRACTOR within the meaning of this Data Processing Agreement is only a service provider that processes the Customer's personal data as a data processor within the meaning of Article 4(8) and Article 28 of the GDPR. The engagement of service providers who merely perform ancillary services without access to personal data (e.g., telecommunications, postal, transportation, or cleaning services) does not constitute a subcontracting relationship within the meaning of this section.
- 5.2 For the SUBCONTRACTORS listed in **Appendix AV4**, whom ALLPLAN engages to provide the SERVICES utilized by the Customer in each case, the Customer's consent is deemed to have been granted. ALLPLAN is entitled to update with the SUBCONTRACTORS listed in Appendix AV4 by providing written notice or by referring to a current overview.
- 5.3 The parties agree that ALLPLAN is generally entitled to engage data processors from among the companies belonging to the Nemetschek Group. This means that all affiliated companies of Nemetschek SE may be used as permissible and approved data processors.
- 5.4 ALLPLAN may engage additional and/or different SUBCONTRACTORS to provide the SERVICES, provided that ALLPLAN notifies the Customer in writing of the intended addition or replacement of SUBCONTRACTORS and the Customer does not object to the intended addition or replacement, at least in writing, within a period of four weeks from receipt of the notification. If no objection to the intended addition or replacement is raised within the specified period, this shall be deemed approval by the Customer. The customer may refuse approval

of the engagement of additional SUBCONTRACTORS or the replacement of existing ones only for good cause; good cause exists, in particular, if the customer has concrete evidence that the proposed SUBCONTRACTOR does not comply with the requirements of the GDPR or applicable data protection law or with appropriate security standards. The objection must be based on specific data protection or security-related grounds. If the customer raises an objection within the specified time limit, ALLPLAN will assess whether the relevant SERVICE can be provided without the intended SUBCONTRACTOR or by using another SUBCONTRACTOR that is equivalent in terms of scope of services, security, and data protection. ALLPLAN shall immediately notify the customer of the result and the next steps and shall decide, at its discretion, whether the affected SERVICE will be provided without the designated SUBCONTRACTOR or by using an equivalent SUBCONTRACTOR. The remaining scope of services and compensation structure shall remain unchanged. If the affected SERVICE cannot be provided without the designated SUBCONTRACTOR nor switched to a SUBCONTRACTOR that is equivalent in terms of scope of services, security, and data protection, the Customer may terminate the affected SERVICE or portion of the service with reasonable notice. Termination of the entire MAIN CONTRACT is permitted only if partial termination is technically or economically impossible or would be unreasonable for the Customer. The right to extraordinary termination for good cause remains unaffected. Upon termination of the relevant SERVICE, the existing provisions regarding the deletion and return of personal data shall apply accordingly.

- 5.5 ALLPLAN shall ensure that only those SUBCONTRACTORS are engaged who provide sufficient guarantees that appropriate technical and organizational measures are in place so that the processing of the customer's personal data is carried out in accordance with the requirements of the GDPR and applicable national data protection laws, and that the protection of the rights of data subjects is ensured. ALLPLAN carefully selects a SUBCONTRACTOR, paying particular attention to the adequacy of the technical and organizational measures implemented by the SUBCONTRACTOR, and will regularly verify the SUBCONTRACTOR's compliance with statutory and contractual data protection requirements.
- 5.6 ALLPLAN shall ensure that the agreement between ALLPLAN and the SUBCONTRACTOR is set forth in a contract that contains at least the same data protection obligations for the SUBCONTRACTOR as those specified for ALLPLAN in this Data Processing Agreement and guarantees a substantially equivalent level of protection for the processing of personal data. ALLPLAN also ensures that the SUBCONTRACTOR engages additional subprocessors only by imposing data protection obligations that guarantee a level of protection comparable to that provided by this Data Processing Agreement. ALLPLAN remains responsible to the Customer for the compliance of these additional subprocessors with their obligations.
- 5.7 The provisions in Section 5 also apply if a SUBCONTRACTOR or another subprocessor located in a third country is involved. The Customer agrees to cooperate to the extent necessary in fulfilling the requirements under Articles 45, 46, and—to the extent applicable in exceptional cases—Article 49 of the GDPR.
- 5.8 ALLPLAN remains responsible to the Customer for compliance with the obligations under this Data Processing Agreement and is liable to the Customer if the SUBCONTRACTOR fails to fulfill its data protection obligations.

6. Location of Data Processing

ALLPLAN will provide the SERVICES in Germany or from the service locations agreed upon with the Customer in the respective MAIN AGREEMENT. Data processing in a third country shall take place exclusively in accordance with the relevant applicable legal provisions of the European Union. ALLPLAN will enter into a contract with another processor that corresponds in content to this Agreement, incorporating the EU Standard Contractual Clauses for the transfer of personal data to processors under Module 3 in accordance with Commission Implementing Decision (EU) 2021/914 of June 4, June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council in third countries that do not provide an adequate level of data protection, or ensure that the requirements of Art. 45 GDPR or Art. 46 of the GDPR are otherwise met. Upon request, ALLPLAN will provide the customer with a copy of the relevant standard contractual clauses, provided that this does not conflict with any statutory confidentiality obligations or the legitimate interests of third parties. The customer agrees to cooperate to the extent necessary to fulfill the requirements.

7. Liability

The liability of the PARTIES toward data subjects is governed by Article 82 of the GDPR. This does not affect ALLPLAN's liability toward the Customer for breach of obligations under this Data Processing Agreement or the MAIN AGREEMENT.

8. Final Provisions

- 8.1 There are no oral or written side agreements to this AV Agreement. The PARTIES agree that the Customer's "General Terms and Conditions" do not apply to this AV Agreement.
- 8.2 All amendments to this AV Agreement must be made in writing (including electronic form). This also applies to any waiver of this written form requirement itself.
- 8.3 In the event of conflicts or contradictions between the provisions of this General Terms and Conditions Agreement and other agreements between the PARTIES, this General Terms and Conditions Agreement shall take precedence with regard to the PARTIES' data protection obligations concerning the processing of personal data on behalf of the Customer.
- 8.4 This General Terms and Conditions Agreement is governed by German law. The exclusive venue for all disputes arising from or in connection with this General Terms and Conditions Agreement is Munich (Munich Regional Court I).
- 8.5 Should individual provisions of this General Terms and Conditions Agreement prove to be wholly or partially invalid or unenforceable, or become invalid or unenforceable as a result of changes in legislation after the conclusion of the agreement, the validity of the remaining provisions shall remain unaffected. The invalid or unenforceable provision shall be replaced by a valid and enforceable provision that most closely approximates the intent and purpose of the invalid provision.

Appendix AV1
Overview of SERVICES

- ALLPLAN Cloud Services
- ALLPLAN Campus
- ALLPLAN Connect
- ALLPLAN Subscription and ALLPLAN Serviceplus for all ALLPLAN products (currently Allplan, FRILO, DC software, SCIA, SDS2)

Appendix AV2
Details of Data Processing

1. Nature and Purpose of Data Processing

Main Contract	Category of the SERVICE	Description of the SERVICE	Type and Purpose
ALLPLAN Cloud Services	Software as a Service (SaaS)	ALLPLAN Cloud comprises SaaS collaboration solutions that enable users to jointly view models, organize and edit them, and access documents. Storage space and computing capacity are provided for the use of ALLPLAN Cloud Services and their features (such as Bimplus, Share, Exchange, Workgroup Manager, as well as additional and specialized tools for collaboration, plan management, and structural engineering). User data is stored or archived for the duration of the contract and deleted upon its expiration.	Collection, Storage, Archiving, Deletion. With ALLPLAN Bimplus, users can manage their projects by selecting participants via invitation to use ALLPLAN Bimplus and assigning rights and roles to those participants. Users can collaborate by creating, assigning, and managing tasks and accessing project data anywhere, anytime, and on any device. ALLPLAN Share allows project participants to work on the same project in ALLPLAN CAD regardless of their location. Different access rights can also be assigned to various project participants. ALLPLAN Exchange enables users to manage their drawings digitally and centrally. Users can distribute their plans to other project participants, version them, download them, track their distribution, and evaluate and document them in project-based reports. Furthermore, users can manage all project participants and automatically notify them via email in various languages.
ALLPLAN Campus	Web Portal	Provision of storage space and computing capacity for the use of ALLPLAN Campus and its features.	Collection, storage, archiving, and deletion. ALLPLAN Campus is a web portal for students, faculty, trainees, and schoolchildren. The web platform is available in various languages at and provides registered users with free access to ALLPLAN products. To do so, users must register and verify their

			identity in order to obtain a student license (or a license for educational purposes) or to use the portal.
ALLPLAN Connect	Web Portal	Provision of storage space and computing capacity for the use of ALLPLAN Connect and its features.	Collection, storage, archiving, deletion. ALLPLAN Connect offers users a free portfolio of information and features that enable them to organize themselves internally. These include a user forum, a chat, and a bulletin board for interacting with other users; a job board for recruiting new employees; and an AI-powered voice assistant (AI Assistant) that answers users' questions about products and services. In addition, Connect handles the management of Allplan licenses. The customer's license administrator can assign the purchased licenses to different users via Connect.
Subscription and Serviceplus Services for ALLPLAN software products	Maintenance and Support Services	Provision of support services (via phone, email, and remote support) for users of ALLPLAN software products.	Organization, sorting, storage, adaptation or modification, retrieval, querying, use, deletion. It cannot be ruled out that individuals employed by ALLPLAN or commissioned by ALLPLAN may come into contact with the user's personal data while providing support services via remote maintenance. Specifically: • Assisting users with software installation and license activation; • Assisting users with the use of the software; • Analyzing error situations and operational disruptions in the software; • Resolving errors in the software.

2. Types and Categories of Personal Data and Categories of Data Subjects

Main Contract	Type of personal data	Categories of data subjects
---------------	-----------------------	-----------------------------

ALLPLAN Cloud Services	☒ Master Data ☒ Address Data ☒ Other data that a customer enters or provides when using the SERVICE.	☒ Users ☒ Employees of users ☒ Users' customers ☒ Users' business partners ☒ Users' suppliers
ALLPLAN Campus	☒ Master data ☒ Address data ☒ Other data that a customer enters or provides when using the SERVICE	☒ Users (teachers, trainees, high school students, and college students)
ALLPLAN Connect	☒ Master data ☒ Address data ☒ Other data that a customer enters or provides when using the SERVICE or that is processed through the use of the SERVICE (user forum, chat, bulletin board: input data/posts; AI chatbot (e.g., AI Coach): input data (prompts), output data (responses)).	☒ Users ☒ Employees of users ☒ Users' customers ☒ Users' business partners ☒ Users' suppliers
ALLPLAN Subscription, ALLPLAN Serviceplus for all ALLPLAN software products	☒ Master data ☒ Address data ☒ Other data that may be relevant in the context of providing maintenance and support services	☒ Users ☒ Employees of users ☒ Users' customers ☒ Users' business partners ☒ Users' suppliers

Appendix AV3

Technical and Organizational Measures

A. ISO/IEC 27001:2022 / Art. 32 GDPR

The data processor's Information Security Management System (ISMS) is certified to ISO/IEC 27001:2022. The certification covers the scope relevant to the provision of services, including the systems and processes used for this purpose and, where applicable, data center and hosting services. Appropriate proof of certification will be provided to the data controller upon request. Measures under the ISMS include systematic risk management, strict access controls, regular data backups, encryption of sensitive data, and comprehensive monitoring of security-related events. In addition, vulnerability and patch management are carried out on an ongoing basis, and security incidents are recorded and addressed as part of an incident management process. Furthermore, measures for secure software development are implemented. Regular audits and reviews ensure continuous improvement of the security level.

Taking into account the state of the art, the costs of implementation, as well as the nature, scope, context, and purposes of the processing, and the varying likelihood and severity of the risks to the rights and freedoms of data subjects, the technical and organizational measures are selected and further developed in such a way as to ensure a level of protection appropriate to the risk in accordance with Article 32 of the GDPR.

This includes, in particular, the ability to ensure the long-term confidentiality, integrity, availability, and resilience of the systems and services related to processing; to quickly restore the availability of personal data and access to it in the event of a physical or technical incident; and to establish a procedure for regularly reviewing, assessing, and evaluating the effectiveness of the technical and organizational measures.

B. ALLPLAN Cloud (Bimplus, Share, Exchange, Workgroup Manager), ALLPLAN Campus, ALLPLAN Connect

1. Access Control

- Implementation and regular review of physical security through a zone-based protection concept, including
 - o surveillance equipment, security personnel, and an access control system
 - o Protection of infrastructure components through security doors and security windows
- Process and documentation for the issuance and return of access credentials, including temporary access
- Escorting visitors
- Access control measures are designed in particular to ensure the confidentiality and integrity of the personal data being processed within the meaning of Article 32(1)(b) of the GDPR.

2. Access Control

- Centralized, standardized user and device management via:
 - o Defined processes for granting, modifying, and revoking access rights
 - o Enforcement of SSO, or at least multi-factor authentication
 - o Additional security measures for privileged access
 - o Management of all mobile devices in a centralized device management system
- Password policy with state-of-the-art minimum requirements for
 - o password complexity
 - o Appropriate cryptographic encryption
 - o Centralized assignment of initial passwords
- Automatic session logout in the event of
 - o inactivity or upon expiration of defined session times
 - o Repeated incorrect entries

- These measures ensure that only authorized persons have access to personal data and the IT systems that process it, thereby achieving a level of protection appropriate to the risk in accordance with Article 32 of the GDPR.

3. Access & Segregation Controls

- Documentation and regular review of user and rights management procedures, including:
 - o Authorization policy
 - o Separation of duties based on the “need-to-know” and “least privilege” principles (segregation of duties)
 - o Consistent multi-tenancy
- Secure configuration and default settings for programs and IT systems, including:
 - o Network segmentation and network diagrams
 - o Segregation of duties (test, development, and production environments)
- Securing external access through technical measures, including:
 - o Intrusion detection system
 - o Secure remote access (use of a Zero Trust Network Access solution)

- The authorization concept, multi-tenancy, and consistent functional separation ensure that the confidentiality and integrity of personal data, as well as the resilience of the systems, are maintained in accordance with Article 32(1)(b) of the GDPR.

4. Data Disclosure Control

- State-of-the-art encryption of data transmission and stored data (electronic transport security)
- Use of an external service provider for document disposal (data bins) and the erasure of data storage media
- Monitoring of access and transmission operations through
 - o logging of accesses
 - o Defining and documenting transmission routes, duration, and data recipients

- Regulations governing the permitted handling and use of data storage media
- The measures implemented to control data disclosure (encryption, logging, regulated transmission routes) help to appropriately minimize risks associated with the transmission of personal data and ensure the security of processing in accordance with Article 32 of the GDPR.

5. Input Control

- Logging and analysis of system usage (entry, modification, deletion)
- Protection of log information, as well as manual or automated monitoring of logs
- Ensuring traceability through time synchronization

-The logging and analysis of entries, modifications, and deletions enable a process for regularly reviewing, assessing, and evaluating the effectiveness of technical and organizational measures, thereby fulfilling the requirements of Article 32(1)(d) of the GDPR.

6. Contractor Oversight

- Drafting of contracts in accordance with legal requirements (Article 28 of the GDPR)
- Identification of existing subcontractors (standardized contract management)
- Regular audits of subcontractors after the contract begins
- Review of the data security policy at subprocessors
- Review of existing IT security certificates for subprocessors
- Selection of contractors based on due diligence criteria
- Conclusion of the necessary data processing agreement

-The structuring of data processing relationships in accordance with Article 28 of the GDPR, as well as the selection and monitoring of subprocessors, ensure that a level of protection appropriate to the risk, as required by Article 32 of the GDPR, is maintained even when processing activities are outsourced.

7. Availability monitoring

- Selection and procurement of cloud services for the provision of our products based on availability criteria (in accordance with ISO standards and the state of the art)
- Backup and recovery strategy in accordance with defined RPO/RTO requirements
 - o Regular and redundant data storage
 - o Regular data recovery tests and logging of results
- Physical security measures for server rooms, including air conditioning and monitoring of temperature and humidity, alarm systems, fire and smoke detectors, and fire extinguishers
- The backup and recovery plan, as well as other measures to maintain system operability, ensure the ability to quickly restore the availability of personal data and access to it in the event of a physical or technical incident (Art. 32(1)(c) GDPR).

8. Malware protection, vulnerability management, and patch management

- Use of software to detect malware and vulnerabilities
- Preventive measures through the use of antivirus protection, firewalls, and spam filters
- System hardening (hardening guidelines) and deactivation of inactive/unused services and ports
- Timely and regular installation of available software and firmware updates
- Retention and analysis of security-related log data
- Through the continuous identification, assessment, and remediation of vulnerabilities, as well as the use of protective mechanisms against malware, the requirement for a level of technical protection appropriate to the risk, as set forth in Article 32 of the GDPR, is met.

9. Incident Management

- Security incident management process, including procedures to comply with the reporting deadlines under Article 33 of the GDPR (72 hours)
 - o Defined and documented reporting channels and emergency plans for handling detected attacks and disruptions
 - o Analysis of security breaches and system disruptions, including an assessment of the risks to data subjects and documentation in accordance with Article 33(5) of the GDPR
 - o Notification of affected parties and the relevant supervisory authorities
- The security incident management process also includes the assessment of risks to the rights and freedoms of data subjects, as well as compliance with reporting and notification obligations to supervisory authorities and data subjects, to the extent required by law. This supports compliance with the requirements for the security of processing pursuant to Article 32 of the GDPR

10. Additional organizational measures

- Operation of an Information Security Management System (ISMS)
- Appointment of a Data Protection Officer
- Appointment of an information security officer
- Awareness-raising and training for employees
- Confidentiality obligations for employees, as well as third parties and data processors
- Establishing guidelines for the permissible personal use of company resources
- Clean Desk and Clear Screen Policy
- Information classification
- Implementation of a data retention policy with defined retention periods, procedures, and responsibilities
- Processes for safeguarding data subjects' rights (Art. 15–22 GDPR)
- Implementation of Privacy by Design and Privacy by Default (Art. 25 GDPR): **Privacy by Design / Privacy by Default**

To the extent that the processor, in the course of providing services, has influence over the design, selection, configuration, or operation of systems, applications, or processes used for the processing of personal data, it shall take into account, to an appropriate extent, the principles of data protection through technical design

and through privacy-friendly default settings pursuant to Art. 25 GDPR. This includes, in particular—to the extent technically feasible and taking into account the nature, scope, context, and purposes of the processing—the implementation of measures for data minimization, access restriction based on the need-to-know principle, privacy-friendly default settings, logging, storage limitation, and the secure erasure of personal data.

- The organizational measures described (ISMS, training, obligations, guidelines) specify the obligation of the controller and the processor to take appropriate organizational measures to demonstrate and permanently ensure compliance with data protection principles and the security of processing in accordance with Articles 24 and 32 of the GDPR.
-
- C. **ALLPLAN, FRILO, DC-Software Subscription, and ALLPLAN, FRILO, DC-Software Serviceplus: REMOTE ACCESS (Art. 32 GDPR) in the Context of Remote Maintenance**
 - Data Protection & Compliance Training for All Employees Involved in Remote Maintenance
 - No unsupervised remote maintenance of the client's systems. It is not possible to run the software completely invisibly in the background.
 - Dedicated remote maintenance software with one-time passwords and brute-force protection.
 - Employees can only connect to the client's computer after the client has provided the generated ID and one-time password.
 - The connection servers are located within the European Union, in data centers certified to ISO 27001.
 - Prompt for the user to close all non-essential processes before access
 - End-to-end encryption of video data with no download option for the contractor
 - State-of-the-art end-to-end encryption of connection data.
 - The customer can terminate the session at any time
 - The design of the remote maintenance process (supervised access, one-time passwords, end-to-end encryption, server locations within the EU) serves to minimize risks to the confidentiality and integrity of personal data and thus meets the requirements for a level of protection appropriate to the risk in accordance with Article 32 of the GDPR.

Appendix AV4
Subcontractor

Name and Address	Location of Data Processing	Type of Service / Processing	Duration of Processing
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy 1855 Luxembourg, Luxembourg	Germany	Provision of infrastructure hosting for Allplan Cloud	Term of the main contract
Microsoft Ireland Operations Ltd. Building 3, Carmanhall Road, Sandyford Industrial Estate 18, Dublin, Ireland	Germany	Provision of infrastructure hosting for the Microsoft Azure platform Use of Azure Open AI Services to provide AI applications (e.g., AI Assistant)	Term of the main contract Term of the main contract
Mailjet GmbH Alt-Moabit 2 10557 Berlin, Germany	Belgium Germany	Provision of technical email delivery services for Allplan Cloud, Allplan Connect, and Allplan Campus	Term of the main contract
PlusServer GmbH Venloer Straße 47 50672 Cologne, Germany	Germany	Provision of infrastructure hosting for Allplan Cloud, Allplan Connect, and Allplan Campus	Term of the main contract
Allplan GmbH Konrad-Zuse-Platz 1, 81829 Munich, Germany	Germany	Provision of infrastructure, software services, platforms, and portals, including their further development, maintenance, and technical support	Term of the main contract
Allplan Austria GmbH Urstein S 19 5412 Puch, Austria	Austria	Provision of support for ALLPLAN software products	Term of the main contract
NEVARIS Construction Software GmbH Hanna-Kunath-Straße 3, 28199 Bremen, Germany	Germany	Provision of 2 nd -level support for Nevaris products	Term of the main contract

TeamViewer Germany GmbH Bahnhofsplatz 2 73033 Göppingen, Germany	Germany	Provision of a software solution for performing remote maintenance for Software Subscription and Software Serviceplus contracts	Term of the main contract
Technyx Euro Services S.R.L. (CANAM GROUP) 9 Ionescu Crum Street 500446 Braşov Romania	Romania	Provision of support for ALLPLAN software products	Term of the main contract
Wibu Systems AG Rüppurrerstr. 52-54, 76137 Karlsruhe, Germany	Germany	Provision of second-level support for licensing issues with Allplan Subscription and Allplan Serviceplus	Term of the main contract
10Duke SOFTWARE LIMITED Registered office: 85-87 Bayham St., London, NW1 0AG, United Kingdom	Ireland	License management, provision of ^{2nd} -level support for licensing issues with ALLPLAN software	Term of the main contract
Solibri Oy Itälahdenkatu 21 A 00210 Helsinki, Finland	Finland	Provision of ^{1st} -level support for Solibri software products	Term of the main contract
SCIA n.v. Corda 2, Kempische Steenweg 309/0.03 3500 Hasselt, Belgium	Belgium Netherlands	Provision of 1st-level support for ALLPLAN software products	Term of the main contract
Bluebeam, Inc. 443 S Raymond Ave, Pasadena, CA, 91105, USA	USA	Provision of first-level support for Bluebeam software products	Term of the main contract
Bluebeam GmbH Konrad-Zuse-Platz 1 81829 Munich, Germany	Germany	Provision of first-level support for Bluebeam software products	Term of the main contract
Nemetschek India Private Limited 4th Floor, B Wing, Purva Summit Building, Whitefield Road, Hitech	India	Provision of support by the Customer Success Team in response to customer inquiries	Term of the main contract

City, Hyderabad- 500081, TS, India			
Nemetschek SE Konrad-Zuse-Platz 1, 81829 Munich, Germany	Germany	Provision of infrastructure hosting for AI applications	Term of the main contract
ACI Axel Christmann Ingenieurtechnik GmbH Paul-Gerhardt-Allee 46, 81245 Munich, Germany	Germany	Provision of support for ALLPLAN software products	Term of the main contract
Allplan France 1 avenue du Général De Gaulle – Tour Hyfive 92800 PUTEAUX, France	France	Provision of support for ALLPLAN software products	Term of the main contract
ALLPLAN Slovensko s.r.o. Bajkalská 19B, 821 01, Bratislava, Slovakia	Slovakia	Provision of support for ALLPLAN software products	Term of the main contract
ALLPLAN Česko s.r.o. Evropská 2590/33c, 160 00 Prague 6, Czech Republic	Czech Republic	Provision of support for ALLPLAN software products	Term of the main contract
Design Data Corp. (d/b/a Allplan and SDS2) 8333 Glynoaks Drive, Suite 200, Lincoln, NE 68516, USA	USA	Provision of support for ALLPLAN software products	Term of the main contract
Allplan Systems Espana S.A. Calle Raimundo Fernández Villaverde 30, Escalera 3, 1st Floor, Office 314, 28003 Madrid	Spain	Provision of support for ALLPLAN software products	Term of the main contract
ALLPLAN Italia S.r.l. is: Via Giovanni Battista Trener 8, 38121 Trento (TN), Italy	Italy	Provision of support for ALLPLAN software products	Term of the main contract
Allplan Schweiz AG Hertistrasse 2c, 8304 Wallisellen, Switzerland	Switzerland	Provision of support for ALLPLAN software products	Term of the main contract

