Annex to the main contract

Agreement on the processing of personal data in the context of the provision of SERVICES (hereinafter: "DPA")

The contracting parties are SCIA N.V. or, if named in the main contract, a company affiliated with SCIA N.V. (hereinafter: "**SCIA**"), and the customer named in the main contract (hereinafter "**the Customer**"), (each individually referred to as "PARTY" and collectively as "PARTIES").

Preamble

This DPA governs the rights and obligations of the PARTIES insofar as personal data is processed by SCIA on behalf of the Customer within the meaning of the applicable data protection law as part of the provision of services in accordance with the terms of use and license conditions or other written or electronic agreements between SCIA and the Customer (hereinafter: "MAIN AGREEMENT") regarding the use of the license platform, the provision of remote maintenance and/or the use of online services (hereinafter: "SERVICES").
This DPA forms an integral part of the MAIN AGREEMENT concluded between the PARTIES. SCIA undertakes the obligations described in this DPA towards all customers who conclude a MAIN CONTRACT with SCIA for the provision of one of the SERVICES listed in **Annex DPA 1** to this DPA.

Updates
If a customer renews or acquires a SERVICE, the provisions of this DPA in force at that time shall apply and shall remain unchanged during the term of this SERVICE.

Electronic notifications
SCIA may provide the customer with information and notifications about SERVICES by e-mail or via the respective SERVICE itself. A notification is deemed to have been given on the date on which it was made available by SCIA.

Earlier versions of this DPA
The provisions of this DPA apply to the currently available SERVICES. Customers can request earlier versions of the DPA from SCIA.

For the purposes of this DPA, the terms "**supervisory authority**", "**processor**", "**data subject**", "**third country**", "**personal data**", "**processing"**, "**controller**" and "**personal data breach**" shall each have the meaning ascribed to them in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - "**GDPR**").

1. Object and duration of processing

1.1 SCIA shall provide the Customer with the SERVICES agreed in the respective MAIN CONTRACT. Insofar as SCIA receives personal data for processing on behalf of the Customer and/or collects or otherwise processes personal data on behalf of the Customer, the Customer is deemed to be the controller and SCIA is deemed to be the processor within the meaning of the GDPR. This DPA -governs the rights and obligations of the PARTIES in this regard.

1.2 As an integral part of the MAIN AGREEMENT, this DPA shall enter into force upon conclusion of the respective MAIN AGREEMENT and shall end upon its termination. The right of each PARTY to terminate this DPA for good cause shall remain unaffected. Good cause entitling SCIA to terminate this DPA exists in particular if there is a current or future governmental regulation or obligation that subjects SCIA to a regulation or requirement that is not generally applicable, which makes it difficult for SCIA to continue the SERVICE without modification and/or causes SCIA to believe that this DPA or SERVICE may be in conflict with such a requirement or obligation.

1.3 If the processing of personal data by SCIA is necessary for the fulfilment of the MAIN CONTRACT or is required by law, for example with regard to the disclosure of personal data to the Customer, after termination of this DPA, this DPA shall continue to apply until the MAIN CONTRACT has been fully fulfilled.

2. Type and purpose of processing, categories of personal data and categories of data subjects

2.1 SCIA processes personal data exclusively on behalf of and in accordance with the instructions of the Customer and only to the extent necessary to provide the SERVICES under the MAIN CONTRACT. The nature and purpose of the processing to be performed by SCIA for the Customer are set out in the MAIN CONTRACT and its annexes and in **Annex DPA 2** to this DPA.

2.2 The type of personal data processed by SCIA under this DPA on behalf of the customer and the categories of data subjects are set out in **Annex DPA 2** to this DPA.

3. Obligations of the Customer

3.1 The Customer is solely responsible for compliance with the legal provisions of the GDPR and the applicable national data protection laws applicable to the Customer and, in particular, for assessing the permissibility of the commissioned processing and for safeguarding the rights of data subjects in accordance with Art. 12 to 22 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 issued verbally; verbal instructions must be confirmed by the Customer immediately in writing or in a documented electronic format.

4. Duties of SCIA

4.1 Compliance with the applicable data protection laws

(a) SCIA undertakes to comply with the applicable provisions of the GDPR and the applicable national data protection laws.

Further information can be found in the data protection information on the SCIA website Privacy policy

4.2 Processing on behalf of the Customer

(a) SCIA processes personal data exclusively in accordance with the provisions of this DPA and - also in case of a potential transfer of personal data to a third country or an international organisation - in accordance with the documented instructions of the Customer, unless SCIA is obliged to act differently by the law of the European Union or the Member States to which SCIA is subject. In such a case, SCIA will notify the Customer of these legal requirements prior to processing, unless the law in question prohibits such notification due to an important public interest.

(b) The MAIN CONTRACT and this DPA are to be understood as instructions. Within the scope of the product-specific parameters, the Customer determines the type and scope of processing by the type of use of the respective SERVICE and by selecting the available options, e.g. with regard to the scope and type of data to be processed.

(c) SCIA will inform the Customer immediately if SCIA is of the opinion that an instruction violates the provisions of the GDPR or applicable national data protection laws. SCIA is authorised to suspend the implementation of the relevant instruction until it is confirmed or amended by the Customer. The PARTIES agree that the responsibility for the processing of personal data in accordance with the instructions lies solely with the Customer.

4.3 Data security and confidentiality

(a) SCIA shall take appropriate technical and organisational measures to ensure that the processing complies with the requirements of the applicable data protection laws and that the rights of the data subjects are protected. The measures must ensure a level of data security appropriate to the risks to

the rights and freedoms of the data subjects. In particular, SCIA shall design its internal organisation 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, unauthorised disclosure or access.

(b) The technical and organisational measures to be taken by SCIA for the respective SERVICES include at least the measures described in Annex DPA 3 of this DPA. SCIA shall review, assess and evaluate the effectiveness of these technical and organisational measures on a regular basis, but at least once a year. SCIA will immediately implement any adjustments that are necessary to maintain data security.

(c) Notwithstanding clauses 4.3 (a) and (b), SCIA may adapt the technical and organisational measures in Annex DPA 3 of this DPA at any time as part of the regular review, assessment and evaluation of the data protection and security concept. However, this is subject to the condition that the amended measures do not fall below the level of protection existing at the time this DPA enters into force. In any case, the level of protection required in accordance with the provisions of the GDPR must be maintained. SCIA shall inform the Customer immediately of any significant adjustments to its technical and organisational measures.

(d) SCIA undertakes to maintain confidentiality when processing personal data. This obligation shall continue to apply after termination of this DPA.

(e) SCIA ensures the reliability and adequate supervision of all persons involved in the processing of personal data and in any case ensures that access to personal data is strictly limited to those persons who need to know such personal data to provide the SERVICES to the Customer. SCIA further ensures that only those persons who have previously been obligated to confidentiality and compliance with data protection requirements in accordance with the statutory requirements can access the personal data.

4.4 Rights of the data subjects

(a) SCIA will inform the Customer immediately if a data subject contacts SCIA directly to assert their rights and will forward the data subject's request to the Customer.

(b) The Customer alone is responsible for responding to requests from affected persons.

(c) However, given the nature of the processing, SCIA will, where possible, support the Customer with appropriate technical and organisational measures to comply with its obligation to respond to requests to exercise the rights of the data subject referred to in Chapter III GDPR. The Customer shall reimburse SCIA for the reasonable expenses incurred by SCIA for the respective support services. The separate remuneration can only be claimed if the customer has requested the corresponding service with knowledge of the specific cost consequences.

4.5 Support for the Customer

(a) SCIA will support the Customer in complying with the obligations set out in Art. 32 to 36 GDPR, taking into account the type of processing and the information available. Costs incurred by SCIA as a result of these support activities are to be reimbursed by the Customer to a reasonable extent. The separate remuneration can only be claimed if the customer has requested the corresponding service with knowledge of the specific cost consequences.

(b) SCIA will inform the Customer immediately as soon as a breach of the protection of personal data becomes known and provide the Customer with the relevant information in accordance with Art. 33 para. 3 GDPR.

(c) SCIA will inform the Customer immediately about inspections or measures by supervisory authorities or other third parties, insofar as these relate to processing under this DPA and SCIA is prohibited from informing the Customer by official order or law. Insofar as SCIA is required to inform the Customer in

accordance with the above provision, SCIA 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) SCIA ensures that all processing activities carried out on behalf of the Customer are documented in accordance with the requirements of Art. 30 para. 2 GDPR.

4.6 Deletion and return of personal data

After termination of this DPA or at the Customer's instruction, SCIA shall, at the Customer's discretion, 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 to store the personal data under Union law or the law of the Member States. If additional costs are incurred due to deviating requirements for the release or deletion of the data, these shall be borne by the customer. The separate remuneration can only be claimed if the customer has requested the corresponding service with knowledge of the specific cost consequences.
SCIA may retain documentation that serves as proof of proper data processing and proper fulfilment of the MAIN CONTRACT even after termination of this DPA.

4.7 Proof of compliance with this DPA and checks by the Customer

(a) SCIA will provide the Customer with all information necessary to demonstrate SCIA's compliance with its obligations under this DPA.

(b) The Customer is authorised to check SCIA's compliance with the provisions of this DPA to a reasonable extent itself or through independent third parties commissioned by it and bound to confidentiality. The customer shall reimburse SCIA for the reasonable expenses incurred by SCIA in the course of an inspection. The separate remuneration can only be claimed if the Customer has called up the corresponding service with knowledge of the specific cost consequences.

(c) The Customer will only carry out checks to the extent necessary. Insofar as SCIA provides proof of the correct implementation of the agreed data protection obligations as described in section 4.3 (b) of this DPA, an inspection shall be limited to spot checks. If an inspection at SCIA should be necessary in individual cases, this must be carried out without avoidable disruption to SCIA's operating processes. Unless otherwise indicated for urgent reasons to be documented by the Customer, inspections will only take place after reasonable advance notice and during SCIA's operating hours and not more frequently than every twelve months.

(d) Insofar as it is possible to inspect confidential information of SCIA within the scope of an inspection, SCIA is authorised to demand a confidentiality obligation from the Customer. Additionally, SCIA is authorised, at its own discretion and taking into account the Customer's legal obligations, not to disclose information if it is confidential with regard to SCIA's business activities or if SCIA would violate legal or contractual regulations by disclosing it.

5. Subcontractors

5.1 SCIA may use other processors to provide the SERVICES (hereinafter: "SUBCONTRACTORS").

5.2 For the SUBCONTRACTORs listed in **Annex DPA 4**, the Customer's authorisation shall be deemed to have been granted for the respective SERVICE used by the Customer.

5.3 SCIA may commission further and/or other SUBCONTRACTORS to provide the SERVICES, provided SCIA informs the Customer of this in text form and the Customer does not object to the intended commissioning at least in text form within a period of four weeks from receipt of the information. If no objection to the intended assignment is raised within the aforementioned period, this shall be deemed to be authorisation by the Customer. The Customer can only refuse to authorise the commissioning of additional or changes to existing SUBCONTRACTORS for good cause. If the Customer objects, SCIA may, at its own discretion, provide the SERVICES without the intended assignment. If the provision of the SERVICES without the intended assignment is not reasonable or possible for SCIA, SCIA must inform the Customer of this immediately. In this case, the Customer may terminate the MAIN CONTRACT between the PARTIES without notice.

5.4 SCIA shall ensure that only those SUBCONTRACTORS are engaged that offer sufficient guarantees that appropriate technical and organisational 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 the protection of the rights of the data subjects is guaranteed. SCIA will carefully select each SUBCONTRACTOR, taking particular account of the suitability of the technical and organisational measures taken by the SUBCONTRACTOR, and will regularly review the SUBCONTRACTOR's compliance with the statutory and contractual data protection requirements.

5.5 SCIA shall ensure that the agreement concluded between SCIA and the SUBCONTRACTOR is governed by a contract that contains at least the same data protection obligations for the SUBCONTRACTOR that are set out in this DPA for SCIA.

5.6 The provisions in Section 5 shall also apply if a SUBCONTRACTOR in a third country is involved. The Customer agrees to cooperate to the extent necessary in the fulfilment of the requirements of Art. 49 GDPR.

5.7 SCIA remains responsible to the Customer for compliance with the obligations arising from this DPA and is liable to the Customer if the SUBCONTRACTOR fails to fulfil its data protection obligations.

6. Place of data processing

SCIA shall provide the SERVICES in Belgium or from the service locations agreed with the Customer in the respective MAIN CONTRACT. Data processing in a third country shall only take place in compliance with the relevant applicable legal provisions of the European Union. SCIA will conclude a contract with another processor that corresponds to the content of this contract, including the EU standard contractual clauses for the transfer of personal data to processors in accordance with Module 3 pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries in accordance with 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 GDPR are otherwise met. The Customer agrees to cooperate in the fulfilment of the requirements to the extent necessary.

7. Liability

The liability of the PARTIES towards data subjects is governed by Art. 82 GDPR. SCIA's liability towards the customer for breach of obligations arising from this DPA or the MAIN AGREEMENT remains unaffected by this.

8. Final provisions

8.1 There are no verbal or written collateral agreements pertaining to this DPA. The PARTIES agree that the "General Terms and Conditions" of the Customer shall not apply to this DPA.

8.2 All amendments to this DPA must be made in text form (including electronic form). This also applies to the waiver of this written form clause itself.

8.3 In the event of any conflict or inconsistency between the provisions of this DPA and any other agreement between the PARTIES, this DPA shall prevail with respect to the data protection obligations of the PARTIES in relation to the processing of personal data on behalf of the Customer.

8.4 This DPA is subject to Belgian law. The sole place of jurisdiction for all disputes arising from and in connection with this DPA is Antwerp.

8.5 Should individual provisions of this DPA prove to be invalid or unenforceable in whole or in part or become invalid or unenforceable as a result of changes in legislation after the conclusion of this DPA, this shall not affect the validity of the remaining provisions. The invalid or unenforceable provision shall be replaced by a valid and enforceable provision that comes as close as possible to the meaning and purpose of the invalid provision.

Annex DPA 1
Overview of SERVICES

- SCIA License Portal
- SCIA Subscription and SCIA Support Services

Annex DPA 2
Details of Processing

1. Nature and purpose of data processing

Main contract	Category of the SERVICE	Description of the SERVICE	Type and purpose
SCIA License Portal	Web portal	Provision of storage space and computing capacity for the use of SCIA License Portal and its functions.	Collection, storage, archiving, deletion. SCIA licences are managed via SCIA License Portal. The user's license administrator assigns the licenses to the different users via SCIA License Portal.
SCIA software Subscription SCIA Support Services	Maintenance and support service	Provision of maintenance and support services for users of SCIA software.	Organisation, classification, storage, adaptation or alteration, retrieval, consultation, use, erasure. It cannot be ruled out that SCIA or persons employed by SCIA or commissioned by SCIA may come into contact with the user's personal data by means of remote maintenance. In detail: • Support for users during the installation of software and activation of the licence; • Support for users when using the software; • Analysing error situations and process faults in the software; • Elimination of errors in the software.

2. Types and categories of personal data and categories of data subjects

Main contract	Type of personal data	Categories of affected persons
SCIA License Portal	☒ Master data ☒ Address data ☒ Other data that a customer enters or provides when using the SERVICE.	☒ User ☒ Employees of users ☒ Customers from users ☒ Business partners of users ☒ Suppliers of users
SCIA Subscription and SCIA Support Services	☒ Master data ☒ Address data ☒ Other data that may be relevant in the context of the provision of maintenance and support services	☒ User ☒ Employees of users ☒ Customers from users ☒ Business partners of users ☒ Suppliers of users

Annex DPA 3
Technical and Organisational measures

A. ISO 27001

Measures in accordance with ISO/IEC 27001 are implemented to ensure information security. These 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 continuously and security incidents are recorded and dealt with as part of an incident management process. Measures for secure software development are also implemented. Regular audits and reviews ensure continuous improvement of the security level.

B. SCIA License Portal

Encryption (Art. 32 para. 1 lit. a) GDPR)

Encryption control

Encrypted data transmission

- Data transmission is encrypted using SSL/TLS or SSH, depending on the area of application
- Administrative access only via separate VPN

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

Access control

- Hosting generally does not take place on-premise at the processor, but only with professional, certified hosting service providers
- Access is only permitted to employees of the hosting service providers and their service providers, provided they have the appropriate authorisation

Entrance control

- Screen locks, incl. password protection
- Functional assignment of user authorisations
- Use of individual passwords, including initial ones
- Blocking of user accounts after multiple incorrect password entries
- Encryption of passwords using at least SHA256 (hashing)
- Passwords are salted
- Two-factor authentication for administrative access
- Password policy with minimum requirements for password complexity
- Process for assigning rights when new employees join the company
- Process for revoking rights when employees change tasks
- Process for withdrawing rights when employees leave the company
- Documentation of the assignment and modification of rights
- Obligation of confidentiality for employees and third parties / processors
- Logging and evaluation of system usage with administrative access
- Central, standardised user administration and login service (single sign-on)

Access control

- Definition of access authorisation, authorisation concept
- Regular review of authorisations
- Partial access options to databases and functions (Read, Write, Execute)
- Regular evaluation of protocols (log files)
- Restriction of free and uncontrolled database queries
- Regulation for restoring data from backups
- Use of security systems:
    - Virus scanner
    - Firewalls
    - SPAM filter
- Clean Desk Policy

Separation control

- Dedicated, separate systems for development, testing and productive operation
- Physical/technical separation of the data storage devices
- Consistent multi-client capability
- Authorisation concept that takes into account the separate processing of data from different users
- Separation of functions
- File separation for databases
- Guidelines and work instructions for employees

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

Input control

- Definition of user authorisations (profiles)
- Differentiated user authorisations (read, change, delete)
- Organisational definition of input responsibilities
- Logging of administrative entries/deletions
- Regulation of access authorisations for log servers (LogAdmin)
- Dedicated log server
- Partial access to data or functions
- Commitment to data secrecy

Integrity (Art. 32 para. 1 lit. c) GDPR)

Availability control

- Backup and recovery concept
- Control of the backup processes
- Regular recovery tests
- Implementation of data backup and backup concepts (daily full backup, goes back several generations, cloud)
- Accessibility of the data backup at any time
- Documentation of the systems
- Existence of a back-up concept
- Regular and controlled verification of backup recoverability
- Software-based protection (virus protection, firewall)

- Contingency plan for data breaches

Resilience and reliability check

- Alternative data centres or other replacement system available
- Data storage on RAID systems (RAID 1 and higher)
- System hardening (deactivation of unnecessary components)
- Immediate and regular activation of available software and firmware updates
- Periodic training and sensitisation measures

Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d) GDPR)

- Regular internal monitoring of security measures
- Responsibilities for data protection and information security are defined
- Management level is regularly informed about the status of data protection and information security as well as possible risks and consequences due to a lack of measures
- If the aforementioned review is negative, the safety measures are adapted, renewed and implemented on a risk-related basis
- Regulation of the circumstances of the authorised private use of company resources
- Regulation of the authorised handling and use of data carriers
- Risk-appropriate classification of personal data
- Reporting channel for events and weaknesses ensured
- Assessment of security breaches and system malfunctions
- Plans for dealing with recognised attacks and disruptions
- Selection of data protection-friendly default settings, insofar as this is relevant for the planned processing operations.

Order control

- Contract design in accordance with legal requirements (Art. 28 GDPR)
- Recording of existing sub-processors (standardised contract management)
- Regular checks on subcontracted processors after the start of the contract
- Review of the data security concept for sub-processors
- Inspection of existing IT security certificates for subcontracted processors
- Selection of contractors from a due diligence perspective
- Conclusion of the necessary agreement on order processing

C. SCIA Subscription and SCIA Software Services:
REMOTE ACCESS as part of remote maintenance:

- Data protection & compliance training for Allplan service personnel
- Dedicated remote maintenance software
- No unattended remote maintenance of the client. It is not possible to run the software completely invisibly in the background.
- Random generation of the remote maintenance ID, verification of the ID for falsification by the service operator.
- Use of one-time passwords
- SCIA Service personnel can only access the customer's computer after the customer has transmitted the generated ID and one-time password.
- The connection servers are located within the European Union, in ISO 27001-certified data centres.
- Brute force protection with exponential increase in waiting times for failed attempts
- Request to the user to close all non-essential processing operations before accessing them
- End-to-end encryption of video data without download option for the contractor
- Encryption based on an RSA public/private key exchange and AES (256-bit) session encoding
- Cancellation option for the user at any time

Annex DPA 4
Subcontractors

Name and address	Place of data processing	Type of service / processing	Duration of processing
Microsoft Ireland Operations Ltd. Building 3, Carmanhall Road Sandyford Industrial Estate 18, Dublin, Ireland	Netherlands	Provision of infrastructure hosting for the Microsoft Azure platform (CRM, Outlook, Azure DevOps, …)	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
Splashtop Inc. 10050 North Wolfe Road, Suite SW2-S260 Cupertino, California 95014	US	Provision of software solution for carrying out remote maintenance for SCIA Software Subscription and Service Contracts	Term of the main contract
10Duke SOFTWARE LIMITED registered office 85-87 Bayham St., London, NW1 0AG Great Britain	Great Britain	SCIA License Portal /Licence management, provision of 2nd level support for SCIA software licensing problems	Term of the main contract
Talkdesk 201 Spear Street, Suite 1100, San Francisco, CA 94105	US	Provision of software communicatin solution for carrying out maintenance for SCIA Software Subscription and Service Contracts	Term of the main contract
IDEA StatiCa s.r.o. Sumavska 35, Brno, 602 00 Czech Republic	Czech Republic	Provision of support for IDEA software products (1st level support)	Term of the main contract