SLASCONE

DATA PROCESSING AGREEMENT (DPA)

SLASCONE GmbH

DPA 10 - 2024

PREAMBLE

This annex specifies the obligations of the contracting parties with regard to data protection arising from the data processing described in detail in the main contract (data processing agreement). It applies to activities related to the contract in which employees of the Contractor or persons commissioned by the Contractor process personal data ("Data") on behalf of the Customer.

1. SCOPE, DURATION AND SPECIFICATION OF DATA PROCESSING

1.1 Annex A and the main contract specify the subject matter as well as the nature and purpose of the processing.

1.2 The duration depends on the provisions of the main contract.

1.3 Explanation of the special right of termination: The Customer may terminate the underlying main contract and the DPA at any time without notice if the Contractor has committed a serious breach of data protection regulations or the provisions of this DPA.

2. SCOPE OF APPLICATION AND RESPONSIBILITY

2.1 The Contractor processes personal data on behalf of the Customer. This includes activities that are specified in the contract and in the service description. Within the framework of this contract, the Customer is solely responsible for compliance with the legal provisions of the data protection laws, in particular for the lawfulness of the data transfer to the Contractor and for the lawfulness of the data processing ("Controller" within the meaning of Art. 4 No. 7 GDPR).

2.2 The instructions are laid down in contract and can then be amended, supplemented or replaced by individual instructions by the Customer in writing or in text form (e.g. e-mail) to the body designated by the Contractor (individual instructions). Instructions that are not provided for in the contract will be treated as an application for a change of benefit. Verbal instructions must be confirmed immediately in writing or in text form by the Customer.

3. OBLIGATIONS OF THE CONTRACTOR

3.1 The Contractor may only process personal data that is the subject of the agreement, within the scope of the agreement and the instructions of the Customer, unless there is an exceptional case within the meaning of Article 28 (3) (a) GDPR and its requirements are met.

3.2 The Contractor shall inform the Customer without delay if it is of the opinion that an instruction violates applicable EU/EEA laws. The Contractor may suspend the implementation of the instruction until it has been confirmed or amended by the Customer.

3.3 The Contractor shall take technical and organizational measures to adequately protect the Customer's data that meet the requirements of the General Data Protection Regulation (Art. 32 GDPR). In particular, the Contractor shall take technical and organizational measures, measured against the risk to the rights and freedoms of the data subjects, which shall ensure the confidentiality, integrity, availability and resilience of the systems and services in connection with the processing in the long term.

The Contractor must document the necessary technical and organizational measures before the start of processing and make them available to the Customer for review. The details of these technical and organizational measures are set out in Annex B.

The technical and organizational measures are subject to technical progress and further development. In this respect, the Contractor is permitted to implement alternative adequate measures. These must be documented accordingly by the Contractor. In doing so, the safety level of the measures listed in Annex B must not be undercut.

3.4 The Contractor shall provide the Customer with appropriate support in fulfilling the enquiries and claims of data subjects in accordance with Chapter III of the GDPR and in complying with the obligations specified in Articles 33 to 36 of the GDPR. (Note: In the GCU, the parties can agree on a remuneration regulation for support services that are not included in the service description or that go beyond the Contractor's legal obligations or are not due to misconduct on the part of the Contractor).
In the event of a claim against the Customer by a data subject with regard to any claims for damages pursuant to Art. 82 GDPR, the Contractor undertakes to support the Customer in defending against the claim within the scope of its possibilities.

3.5 The Contractor guarantees that the employees involved in the processing of the Customer's data and other persons working for the Contractor are prohibited from processing the data outside of the instructions. Furthermore, the Contractor guarantees that the persons responsible for processing the personal data have committed themselves to confidentiality and that this confidentiality obligation continues even after the termination of the assignment.

3.6 The Contractor shall inform the Customer without undue delay if it becomes aware of any breach of the Customer's personal data protection. A data breach notification must contain at least:

- a description of the incident, where possible, specifying the nature of the personal data breach, specifying the categories and approximate number of data subjects, categories affected and the approximate number of personal data records affected
- the name and contact details of the data protection officer or other contact point for further information
- a description of the likely consequences of the reported incident, a description of the measures taken to remedy and, if necessary, Measures to mitigate their possible adverse effects

3.7 The Contractor shall give the Customer the name of the contact person for data protection issues arising within the scope of the contract:
Dr. Ilias Michalarias
Manager

Communication channels to be used for instruction:
support@slascone.com

3.8 The Contractor guarantees to use a procedure for regularly reviewing the effectiveness of the technical and organizational measures to ensure the security of processing (Art. 32 para. 1 lit. d GDPR).

3.9 During the term of the contract, the Contractor shall correct or delete the data subject to the contract on the instructions of the Customer. If it is not possible to delete this data in accordance with data protection regulations, the Contractor shall ensure that the data carriers and documents containing the data subject to the contract are destroyed in accordance with data protection regulations.
Data carriers and processed data handed over to the Processor by the Customer, including copies made.
The Contractor shall correct or delete the data subject to the contract if the Customer instructs this and this is covered by the framework of instructions.

If deletion in accordance with data protection regulations or a corresponding restriction of data processing is not possible, the Contractor shall take over the destruction of data carriers and other materials in accordance with data protection regulations on the basis of an individual order by the Customer or return these data carriers to the Customer, unless already agreed in the contract. (Note: In the contract, the parties can make a remuneration arrangement for this.)

In special cases to be determined by the Customer, storage or handover will take place, remuneration and protective measures for this are to be agreed separately, unless already agreed in the contract.

3.10 Data, data carriers and all documents are to be either surrendered after the end of the agreement at the request (in writing or in text form through email), if they are the property of the Customer, or deleted.
If additional costs arise due to deviating specifications in the release or deletion of the data, these shall be borne by the Customer.

3.11 The Customer and the Contractor will cooperate with the supervisory authority upon request in carrying out their tasks. Immediate information to the Customer about control actions and measures taken by the supervisory authority insofar as they relate to this order. This also applies if an authority investigates the processing of personal data during order processing by the Contractor as part of an administrative offense or criminal procedure. If the Customer is exposed to an inspection by the supervisory authority, an administrative offense or criminal proceedings, the liability claim of a data subject or a third party or another claim in connection with the processing of the order by the Contractor, the Contractor must support him to the best of his ability.

4. OBLIGATIONS OF THE CLIENT

4.1 The Customer shall inform the Contractor immediately and in full if it discovers errors or irregularities in the results of the contract.

4.2 In the event of a claim against the Contractor by a data subject with regard to any claims for damages pursuant to Art. 82 GDPR, the Contractor undertakes to support the Customer in defending against the claim within the scope of its possibilities.

5. DATA SUBJECT REQUESTS

If a data subject contacts the Contractor with requests pursuant to Art. 15 to 21 GDPR, the Contractor shall immediately refer the data subject to the Customer and forward the application to the Customer. The Contractor shall assist the Customer in fulfilling these requests of the data subjects to the extent necessary.

6. DOCUMENTATION OPTIONS

6.1 The Contractor shall prove to the Customer that it has complied with the obligations laid down in this Agreement by appropriate means. The Contractor undertakes to provide the Customer with the documented controls and necessary information upon request. In particular, the implementation of the technical and organizational measures in accordance with Article 32 GDPR must be proven.

6.2 Proof of compliance with the obligations laid down in this contract may be provided by:

- Current attestations, reports or report excerpts from independent bodies (e.g. auditors, auditors, data protection officers, IT security departments, data protection auditors, quality auditors)
- Self-audits
- Suitable certification by IT security or data protection audit (e.g. according to BSI baseline protection, ISO 27001, ISO 27018, ISO 27701)
- Compliance with approved rules of conduct in accordance with Art. 40 GDPR
- certification according to an approved certification procedure in accordance with Art. 42 GDPR
- Agreement between the Customer and the Contractor that proof can also be provided by the following documents / certificates

6.3 Control rights

a) The Contractor undertakes to support the Customer in its audits pursuant to Art. 28 (3) sentence 2 lit. h GDPR to ensure compliance with the provisions on data protection and the contractual agreements to the appropriate and necessary extent.

b) The inspections are carried out by the Customer himself or by a third party commissioned by him. If the third party commissioned by the Customer is in a competitive relationship with the Contractor, the Contractor shall have a right of objection against the latter. Commissioned third parties must be obliged to secrecy by the Customer. The Contractor shall have the right to demand the submission of a separate confidentiality agreement by the commissioned third party. This applies in particular to the submission of declarations of professional or statutory secrecy.

An examination can be carried out in particular by obtaining information and inspecting the stored data and the data processing programs as well as by other measures. Other measures include requesting certifications and reports on data protection audits.

7. OTHER PROCESSORS (SUBCONTRACTORS)

7.1 A subcontractor relationship requiring consent exists if the Contractor commissions other contractors to process personal data as agreed in the contract. The Contractor will enter into agreements with these third parties to the extent necessary to ensure appropriate data protection and information security measures.

7.2 The Customer agrees that the Contractor may use subcontractors. Before using or replacing the subcontractors, the Contractor shall inform the Customer (if necessary, add the deadline and/or regulation for emergency situations here).

7.3 Web hosting of the SLASCONE Licensing & Analytics application incl. storage of customer data (server location EU)

Name and address of the subcontractor	Description
Microsoft Ireland Operations Ltd, One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521 Irland	Web hosting of the SLASCONE Licensing & Analytics application incl. storage of customer data (server location EU)

The Customer may object to the change – within one month – for important reasons under data protection law – vis-à-vis the Contractor. If no objection is made within the deadline, consent to the change is deemed to have been given. If there is an important reason under data protection law, and if an amicable solution is not possible between the parties, the Customer is granted a special right of termination.

7.4 If the Contractor concludes agreements with subcontractors, it is the Contractor's responsibility to transfer its data protection obligations under this contract to the subcontractor.

7.5 If the subcontractor does not comply with its data protection obligations, the first processor is liable to the Customer for compliance with the obligations of that other processor.

8. TRANSFERS TO THIRD COUNTRIES

8.1 The contractually agreed data processing takes place in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. Relocations or data processing in a third country may only take place if the requirements of Art. 44 et seq. GDPR are met.

8.2 One of the following options is used to maintain the appropriate level of protection:

- by an adequacy decision of the Commission (Art. 45 para. 3 GDPR)
- is established by binding internal data protection regulations, including additional protective measures if necessary (Art. 46 para. 2 lit. b in conjunction with 47 GDPR)
- is established by correspondingly modulated standard data protection clauses, including additional protective measures if necessary (Art. 46 para. 2 lit. c and d GDPR)
- is established by approved rules of conduct (Art. 46 para. 2 lit. e in conjunction with 40 GDPR)
- is established by an approved certification mechanism (Art. 46 para. 2 lit. f in conjunction with 42 GDPR)

- The Contractor is entitled to ensure the appropriate level of protection in other ways provided for in Art. 44 et seq. GDPR

8.3 If nothing has been agreed in the contract, processing in a third country is only permissible with the prior consent of the Customer. The Contractor shall inform the Customer in advance of the third country(s) concerned and how the appropriate level of protection within the meaning of Art. 44 et seq. GDPR is ensured for the processing there.

9. LIABILITY

The Customer and Contractor shall be liable to data subjects accordingly
of the regulation made in Art. 82 GDPR.

10. INFORMATION OBLIGATIONS, WRITTEN FORM CLAUSE, CHOICE OF LAW

10.1 If the Customer's data at the Contractor is endangered by attachment or seizure, by insolvency or composition proceedings or by other events or measures of third parties, the Contractor shall inform the Customer thereof immediately. The Contractor shall immediately inform all persons responsible in this context that the sovereignty and ownership of the data lies exclusively with the Customer as the "controller" within the meaning of the General Data Protection Regulation.

10.2 Changes and additions to this Appendix and all its components – including any assurances given by the Contractor – require a written agreement, which may also be made in electronic format (text form), and the express indication that it is a modification or supplement to these Terms and Conditions. This also applies to the waiver of this formal requirement.

10.3 In the event of any contradictions, the provisions of this Annex on data protection shall take precedence over the provisions of the contract. If individual parts of this system are invalid, this does not affect the validity of the rest of the system.

10.4 German law applies.

ANNEX A DETAILS ON DATA PROCESSING

1. DESCRIPTION OF THE PURPOSE AND NATURE OF THE PROCESSING OF PERSONAL DATA

The subject of the data processing agreement is the execution of the following tasks by the Contractor:

The purposes of the processing are all contractual purposes necessary for the provision of the contractually agreed service, which result from the contract itself or further documents relating to the contract. The type of processing includes all types of processing within the meaning of the GDPR, details are set out in the main contract together with annexes or the DPA.

In particular, the following activities are part of the data processing. Storage of the data entered by the Customer via the user interface in a database, reproduction, systematization, tabular and/or graphical evaluation of the data as well as deletion of the data at the request of the Customer, maintenance and hosting of the IT systems, software and databases on which the service is based and the handling of backups.
The Contractor processes personal data on behalf of the Customer. This is done by using SLASCONE Licensing & Analytics, a software solution for license management.

2. CATEGORIES OF DATA SUBJECTS

- Employees (incl. applicants)
- Resellers and their employees
- (End) Customers and their employees

3. TYPE OF PERSONAL DATA

- Contact and identification data: e.g. first and last name, address, country, telephone/mobile, e-mail address, title
- Communication and Network Data: Data generated by the use of a software license.

ANNEX B TECHNICAL AND ORGANIZATIONAL MEASURES (TOM) WITHIN THE MEANING OF ART. 32 GDPR

1. CONFIDENTIALITY PURSUANT TO ART. 32 PARA. 1 LIT. B GDPR

1.1 PHYSICAL ACCESS CONTROL

Measures that are suitable for denying unauthorized persons access to data processing systems with which personal data are processed or used.

All relevant data processing systems are located in Microsoft Azure data centers. Microsoft measures and certifications apply here.

Technical measures	Organizational measures
Manual locking system	Key regulation / list

1.2 LOGICAL ACCESS CONTROL

Measures suitable for preventing data processing systems from being used by unauthorized persons.

Technical measures	Organizational measures
Login with username + password	Managing User Permissions
Firewall	Creating User Profiles
Encryption of notebooks / Tablet	Strong Password Policy
MFA (Multi-Factor Authentication)	Delete/Destroy Policy
Automatic desktop lock	General Policy Privacy and Security
Antivirus	

1.3 AUTHORIZATION CONTROL

Measures to ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified, or removed without authorization during processing, use and after storage.

Technical measures	Organizational measures
Logging of application access, specifically when entering, editing and deleting data	Use of authorization concepts
	Minimum number of administrators
	Management of user rights by administrators

1.4 SEPARATION CONTROL

Measures that ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logical and physical separation of the data.

Technical measures	Organizational measures
Separation of production and test environments	Control via authorization concept
Multi-tenancy of relevant applications	Defining database rights

1.5 PSEUDONYMIZATION (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR)

The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures.

Technical measures	Organizational measures
In the case of pseudonymization: separation of assignment data and preservation in separate and separate secured system (possibly encrypted)	Internal instruction to anonymize / pseudonymize personal data as far as possible in the event of disclosure or even after the expiry of the statutory deletion period

2. INTEGRITY (ART. 32 PARA. 1 LIT. B GDPR)

2.1 DATA TRANSFER CONTROL

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and establish to which entities personal data are intended to be transmitted by data transmission equipment.

Technical measures	**Organizational measures**
Access logging	Disclosure in anonymized or pseudonymized form
Deployment via encrypted Connections such as sftp, https	

2.2 DATA INPUT CONTROL

Measures that ensure that it is possible to check and establish retrospectively whether and by whom personal data has been entered into, modified or removed from data processing systems. Input control is achieved through logging, which can take place at various levels (e.g., operating system, network, firewall, database, application).

Technical measures	**Organizational measures**
Technical logging of the input, Modification and deletion of data	Assignment of rights to enter, change and delete data based on an authorization concept

3. AVAILABILITY AND RESILIENCE (ART. 32 PARA. 1 LIT. B GDPR)

3.1 AVAILABILITY CONTROL

Measures to ensure that personal data is protected against accidental destruction or loss.

All relevant data processing systems are located in Microsoft Azure data centers. Microsoft measures and certifications apply here.

3.2 RECOVERABILITY CONTROL

Measures capable of rapidly restoring the availability of and access to personal data in the event of a physical or technical incident.

All relevant data processing systems are located in Microsoft Azure data centers. Microsoft measures and certifications apply here.

ANNEX C INCIDENT RESPONSE PLAN

This incident response plan is designed to outline procedures for managing and mitigating security incidents for a SaaS (Software-as-a-Service) company. The objective is to provide a structured, efficient, and compliant response to security threats while minimizing impact on customers, services, and the organization. More details can be found at https://support.slascone.com/hc/en-us/articles/22297946221725-INCIDENT-RESPONSE-PLAN-IRP