SLASCONE

Data Processing Agreement (DPA)

May 2026

PREAMBLE

This Data Processing Agreement (“DPA”) forms part of and is incorporated into the Agreement between SLASCONE GmbH (“Provider” or “Processor”) and the customer identified in the applicable Order Form, quotation, offer, subscription confirmation, trial confirmation, or other written agreement (“Customer” or “Controller”).

This DPA applies to the extent Provider processes Personal Data on behalf of Customer in connection with the services.

1. DEFINITIONS AND SCOPE

1.1 Unless otherwise defined in this DPA, capitalized terms have the meanings given in the Agreement. The terms “Personal Data”, “Processing”, “Controller”, “Processor”, “Data Subject”, “Personal Data Breach”, and “Supervisory Authority” shall have the meanings given to them in the GDPR.

1.2 This DPA governs Provider’s Processing of Personal Data on behalf of Customer in connection with the services under the Agreement.

1.3 As between the parties, Customer acts as Controller and Provider acts as Processor with respect to Personal Data Processed on behalf of Customer under this DPA, unless applicable data protection law requires otherwise for a specific Processing activity.

1.4 In the event of any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of such conflict with regard to the Processing of Personal Data on behalf of Customer.

2. SUBJECT MATTER, DURATION, NATURE AND PURPOSE OF PROCESSING

2.1 The subject matter of the Processing is the provision of the services by Provider to Customer under the Agreement.

2.2 This DPA shall remain in effect for as long as Provider Processes Personal Data on behalf of Customer under the Agreement.

2.3 The nature and purpose of the Processing, the categories of Data Subjects, and the categories of Personal Data are described in ANNEX A.

3. CUSTOMER INSTRUCTIONS

3.1 Provider shall Process Personal Data only on documented instructions from Customer, unless otherwise required by applicable law to which Provider is subject. The Agreement, this DPA, and Customer’s use and configuration of the services constitute Customer’s complete and documented instructions as of the effective date of this DPA.

3.2 Customer may issue additional reasonable documented instructions to Provider, provided that such instructions are consistent with the Agreement and this DPA, required for Customer’s compliance with applicable data protection law, and technically feasible. Provider may reject instructions that are unlawful, technically infeasible, or materially outside the agreed scope of the services. Provider may charge reasonable additional fees for implementing additional instructions that fall outside the standard scope of the services, provided that any such additional fees have been approved by Customer in writing in advance.

3.3 If Provider believes that an instruction from Customer infringes applicable data protection law, Provider shall inform Customer without undue delay. Provider may suspend execution of the relevant instruction until Customer confirms or amends it.

3.4 If Provider is required by applicable law to Process Personal Data other than on Customer’s instructions, Provider shall inform Customer of that legal requirement before the Processing, unless that law prohibits such information on important grounds of public interest.

4. PROCESSOR OBLIGATIONS

4.1 Provider shall ensure that persons authorized by Provider to Process Personal Data:
a) are bound by confidentiality obligations or are under an appropriate statutory duty of confidentiality; and
b) access Personal Data only to the extent necessary for the performance of the Agreement and in accordance with Customer's documented instructions.

4.2 Provider shall implement and maintain appropriate technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing, and the risks to the rights and freedoms of natural persons.
The technical and organizational measures applicable as of the effective date of this DPA are described in ANNEX C.

4.3 Provider may update or modify the technical and organizational measures from time to time, provided that such changes do not materially reduce the overall level of security for the Processing covered by this DPA.

4.4 Taking into account the nature of the Processing, Provider shall provide Customer with reasonable assistance, through appropriate technical and organizational measures where possible, to enable Customer to respond to requests for exercising Data Subject rights under applicable data protection law.

If Provider receives a request directly from a Data Subject relating to Personal Data Processed on behalf of Customer, Provider shall, unless legally prohibited, promptly forward the request to Customer. Provider shall not respond to such request except on Customer's documented instructions or as required by applicable law.

4.5 Taking into account the nature of the Processing and the information available to Provider, Provider shall provide reasonable assistance to Customer with Customer's compliance obligations under Articles 32 to 36 GDPR, including with respect to:
a) security of Processing;
b) notification and handling of Personal Data Breaches;
c) data protection impact assessments; and
d) prior consultations with Supervisory Authorities.

4.6 Provider shall notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Personal Data Processed on behalf of Customer and, in any event, no later than forty-eight (48) hours after becoming aware of such Personal Data Breach.
To the extent available to Provider, such notification shall include:
a) a description of the nature of the Personal Data Breach, including, where possible, the categories and approximate number of affected Data Subjects and Personal Data records;
b) the likely consequences of the Personal Data Breach;
c) the measures taken or proposed to address the Personal Data Breach and mitigate its possible adverse effects; and
d) the contact details of a point of contact from whom further information may be obtained.

Provider may provide the information in phases if it is not possible to provide all information at the same time.

4.7 Provider shall make available to Customer all information reasonably necessary to demonstrate compliance with Provider's obligations under this DPA and applicable data protection law.

4.8 Provider shall not sell Personal Data and shall not Process Personal Data for its own purposes other than:
a) as required to provide the services in accordance with the Agreement and Customer's instructions;
b) as required by applicable law; or
c) as otherwise permitted under applicable data protection law where Provider acts as an independent controller for such specific Processing activity.

5. CUSTOMER OBLIGATIONS

5.1 Customer shall be responsible for the lawfulness of the Processing of Personal Data under the Agreement, including:
a) the existence of an appropriate legal basis;
b) the lawfulness of disclosing Personal Data to Provider;
c) the lawfulness of Customer's instructions to Provider; and
d) compliance with Customer's transparency and information obligations toward Data Subjects.

5.2 Customer is responsible for the accuracy, quality, and legality of the Personal Data provided to Provider and for ensuring that Customer does not instruct Provider to Process Personal Data beyond what is necessary for the purposes of the Agreement.

5.3 Customer is responsible for configuring and using the services in a manner consistent with applicable data protection law, including with respect to user access, retention settings, and deletion requests.

5.4 Customer shall provide Provider with reasonable cooperation and information required for Provider to comply with lawful instructions under this DPA.

6. SUBPROCESSORS

6.1 Customer grants Provider a general authorization to engage subprocessors for the Processing of Personal Data on behalf of Customer in connection with the services.

6.2 The subprocessors authorized as of the effective date of this DPA are listed in ANNEX B.

6.3 Provider may add or replace subprocessors from time to time. Provider shall inform Customer in advance of any intended addition or replacement of a subprocessor by updating ANNEX B or by another reasonable notice mechanism.

6.4 Customer may object to a new subprocessor on reasonable grounds relating to data protection within thirty (30) days after receipt of notice. If Customer objects, the parties shall discuss in good faith whether a commercially reasonable solution can be achieved.
If no such solution is reasonably available, Provider may either:
a) not appoint the relevant subprocessor for Customer;
b) allow Customer to suspend or terminate the affected part of the services; or
c) if the new subprocessor is essential for the continued provision of the services, terminate the affected services in accordance with the Agreement.

6.5 Provider shall impose on each subprocessor data protection obligations that are no less protective than those set out in this DPA to the extent applicable to the services performed by that subprocessor.

6.6 Provider shall remain responsible for the performance of its subprocessors' obligations to the extent required by applicable data protection law.

7. INTERNATIONAL TRANSFERS

7.1 Provider shall not transfer Personal Data to a country outside the European Economic Area unless such transfer is carried out in compliance with applicable data protection law.

7.2 Where Provider or a subprocessor transfers Personal Data to a country outside the European Economic Area, Provider shall ensure that an appropriate transfer mechanism under applicable data protection law is in place, such as:
a) an adequacy decision;
b) the EU Standard Contractual Clauses; or
c) another legally recognized transfer mechanism.

7.3 Where required by applicable data protection law, Provider shall implement appropriate supplementary measures in connection with international transfers.

7.4 Upon Customer's reasonable request, Provider shall provide information on the transfer mechanism relied upon for relevant international transfers, to the extent legally and contractually permitted.

8. AUDIT AND DEMONSTRATION OF COMPLIANCE

8.1 Provider may satisfy its audit and information obligations under this DPA by providing:
a) current certifications, attestations, reports or excerpts from reports from independent auditors;
b) summaries of relevant security and compliance documentation;
c) responses to reasonable due diligence questionnaires; and
d) other information reasonably required to demonstrate compliance with this DPA.

Provider may also make available, as appropriate, information regarding relevant certifications and independent assessments, including ISO/IEC 27001 certification information, in order to support Customer's assessment of Provider's compliance and technical and organizational measures.

8.2 If the information provided under Section 8.1 is insufficient to demonstrate compliance with this DPA, Customer may request an audit by itself or by an independent third party bound by confidentiality obligations, subject to the following conditions:
a) at least thirty (30) days' prior written notice, unless a shorter period is required by a Supervisory Authority;
b) no more than once per calendar year, unless a Personal Data Breach, material compliance issue, or Supervisory Authority request justifies an additional audit;
c) the audit must be limited in scope to information relevant to Customer's Processing under this DPA;
d) the audit must be conducted during normal business hours and in a manner that avoids unreasonable disruption to Provider's business;
e) Customer shall not gain access to information relating to other customers of Provider; and

f) Customer shall bear its own costs and reimburse Provider's reasonable internal and external costs incurred in connection with the audit, except where the audit demonstrates a material breach of this DPA by Provider.

8.3 Provider may object to an auditor that is, in Provider's reasonable opinion, not suitably qualified or independent, or is a direct competitor of Provider.

9. RETURN AND DELETION OF PERSONAL DATA

9.1 Upon termination or expiry of the Agreement, Provider shall, at Customer's choice, delete or return Personal Data Processed on behalf of Customer, unless applicable law requires storage of the Personal Data.

9.2 The practical process, timing, and format for data export, return, deletion, and any related retention periods may be further described in the Agreement, the applicable documentation, or Provider's standard offboarding procedures, provided that such procedures remain consistent with applicable data protection law, this DPA, and the Agreement.

9.3 Provider may retain Personal Data contained in backup systems for a limited period in accordance with Provider's standard backup retention practices, provided that such retained Personal Data remains protected in accordance with this DPA and is deleted in the ordinary course.

9.4 To the extent Provider is required by applicable law to retain Personal Data, Provider shall continue to protect such Personal Data in accordance with this DPA and shall not further Process it except as required by applicable law.

10. COOPERATION WITH SUPERVISORY AUTHORITIES

10.1 Provider shall, to the extent required by applicable data protection law, cooperate with Supervisory Authorities in relation to the Processing of Personal Data covered by this DPA and shall inform Customer without undue delay of any inquiry, inspection, or other binding measure by a Supervisory Authority relating specifically to Customer's Personal Data, unless legally prohibited from doing so.

11. CONTACT POINT

11.1 Provider's contact point for data protection matters under this DPA is:
SLASCONE GmbH
Email: support@slascone.com
Provider may update the contact details from time to time by notice to Customer.

12. LIABILITY

12.1 The liability of each party under this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement, except to the extent such exclusions or limitations are prohibited by applicable data protection law.

12.2 Nothing in this DPA shall be construed to limit the rights of Data Subjects under applicable data protection law.

13. MISCELLANEOUS

13.1 This DPA shall be governed by the law governing the Agreement, unless applicable data protection law requires otherwise.

13.2 Provider may update this DPA from time to time to reflect changes in applicable data protection law, regulatory guidance, subprocessors, or non-material administrative changes to Provider's Processing practices, provided that such updates do not materially reduce the level of protection afforded to Personal Data under this DPA without Customer's agreement where required by applicable law.

13.3 If any provision of this DPA is held invalid or unenforceable, the remaining provisions shall remain in full force and effect.

ANNEX A DETAILS OF PROCESSING

1. Subject Matter

Provision of the SLASCONE Licensing & Analytics services and related hosting, support, maintenance, backup, monitoring, and technical administration.

2. Nature of Processing

The Processing may include, as applicable:

- collection
- recording
- organization
- structuring
- storage
- adaptation or alteration
- retrieval
- consultation
- use
- disclosure by transmission where necessary for the provision of the services
- restriction
- deletion
- destruction

3. Purpose of Processing

Processing necessary for the provision, operation, support, security, maintenance, and improvement of the contractual services under the Agreement.

4. Categories of Data Subjects

Depending on Customer's use of the services, Data Subjects may include:

- Customer employees and users
- Customer prospects, resellers, partners, and their employees
- Customer end customers and their employees
- other individuals whose Personal Data Customer chooses to upload to or process through the services

5. Categories of Personal Data

Depending on Customer's use of the services, Personal Data may include:

- identification data, such as first and last name

- contact data, such as business email address, postal address, telephone number, company, country, and title
- account and user data
- licensing and entitlement data
- usage, communication, device, and network-related data generated in connection with the use of the services
- support-related information submitted by Customer
- any other Personal Data that Customer chooses to upload to or process through the services

6. Special Categories of Personal Data

Provider does not require Customer to submit special categories of Personal Data for ordinary use of the services. Customer shall not upload special categories of Personal Data unless this has been expressly agreed in writing and appropriate safeguards have been implemented.

7. Frequency of Processing

Continuous or ad hoc, depending on Customer's use of the services during the term of the Agreement.

ANNEX B AUTHORIZED SUBPROCESSORS

As of the effective date of this DPA, Provider uses the following subprocessors for the services:

Name and address of the subprocessor	**Purpose**	**Location / Region**
Microsoft Ireland Operations Limited, One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521 Ireland	Cloud hosting, infrastructure, storage, and related platform services for SLASCONE Licensing & Analytics	Hosting region used for the relevant Customer environment, including the European Economic Area or the United States, as applicable.

Provider may update this Annex in accordance with Section 6 of this DPA.

ANNEX C TECHNICAL AND ORGANIZATIONAL MEASURES (TOM)

Provider implements and maintains technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. Such measures are designed taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing, and the risks to the rights and freedoms of natural persons.

Provider maintains and further develops its information security and data protection measures as part of its overall security governance and operational processes. Provider may also make available, as appropriate, information regarding relevant certifications and independent assessments, including ISO/IEC 27001 certification information, in order to support Customer's assessment of Provider's technical and organizational measures. For the avoidance of doubt, any such certification information supplements, but does not replace, the measures described in this Annex.

1. Access Control

Provider implements measures intended to prevent unauthorized persons from gaining access to systems in which Personal Data is Processed. Such measures may include, as applicable:

- role-based access controls
- least-privilege principles for internal access
- authentication controls for administrative access
- multi-factor authentication for privileged access where applicable
- processes for granting, reviewing, modifying, and removing access rights
- logical access restrictions to production systems and administrative tools

2. System Security

Provider implements measures intended to protect systems and services against unauthorized access, malicious activity, and technical vulnerabilities. Such measures may include, as applicable:

- network security controls such as firewalls, traffic filtering, and segmentation where appropriate
- secure configuration and hardening practices
- endpoint protection and malware protection for managed devices where applicable
- vulnerability management processes
- security patching and update procedures
- controlled administrative access to infrastructure and service components

3. Encryption and Transmission Security

Provider implements measures intended to protect Personal Data during transmission and storage. Such measures may include, as applicable:

- encryption in transit using industry-standard protocols where supported
- encryption at rest where supported by the underlying infrastructure and service configuration
- secure remote access methods where remote administration is required

- key and secret handling processes appropriate to the services and infrastructure used

4. Authorization and Separation

Provider implements measures intended to ensure that Personal Data is Processed only by authorized personnel and within the intended scope. Such measures may include, as applicable:

- separation of production and non-production environments where appropriate
- tenant separation and logical segregation mechanisms within the service architecture
- administrative controls for database, application, and infrastructure permissions
- separation of duties where appropriate for critical functions

5. Logging and Monitoring

Provider implements measures intended to detect, investigate, and respond to operational and security-related events. Such measures may include, as applicable:

- logging of relevant administrative, operational, and security events where appropriate
- monitoring mechanisms intended to detect operational or security anomalies
- alerting and escalation processes for relevant incidents
- review and retention of logs in accordance with operational and security requirements

6. Availability and Resilience

Provider implements measures intended to maintain the availability and resilience of the services and the Personal Data Processed through them. Such measures may include, as applicable:

- backup and recovery processes appropriate to the service
- resilience and continuity measures based on the underlying cloud infrastructure and Provider's operational procedures
- procedures for restoring availability and access to Personal Data following an incident
- testing or validation of relevant recovery and restoration processes where appropriate

7. Confidentiality and Personnel Measures

Provider implements measures intended to ensure that personnel handling Personal Data are appropriately authorized and informed. Such measures may include, as applicable:

- confidentiality commitments or statutory confidentiality obligations for personnel with access to Personal Data
- training and awareness measures on privacy and security
- onboarding and offboarding procedures for personnel access
- review of personnel access rights where appropriate

8. Development and Change Management

Provider implements measures intended to ensure that changes to systems and software are controlled and appropriately reviewed. Such measures may include, as applicable:

- controlled deployment and change-management procedures
- testing and validation processes for relevant changes

- segregation of development, testing, and production activities where appropriate
- procedures for managing and approving changes affecting security or Processing operations

9. Vendor and Subprocessor Management

Provider implements measures intended to ensure that relevant subprocessors and vendors are subject to appropriate oversight. Such measures may include, as applicable:

- due diligence and selection procedures for relevant subprocessors and service providers
- contractual data protection and security obligations imposed on subprocessors as required by law
- review of relevant subprocessor or vendor security information where appropriate

10. Review and Improvement

Provider implements measures intended to ensure that technical and organizational measures remain appropriate over time. Such measures may include, as applicable:

- periodic review and update of security measures
- adaptation of measures in light of technical developments, risk assessments, operational experience, and legal requirements
- review of relevant incidents and follow-up improvements where appropriate

For the avoidance of doubt, certain technical and organizational measures are implemented through Provider's cloud infrastructure providers and related managed services used for the operation of the services, including Microsoft Azure where applicable.