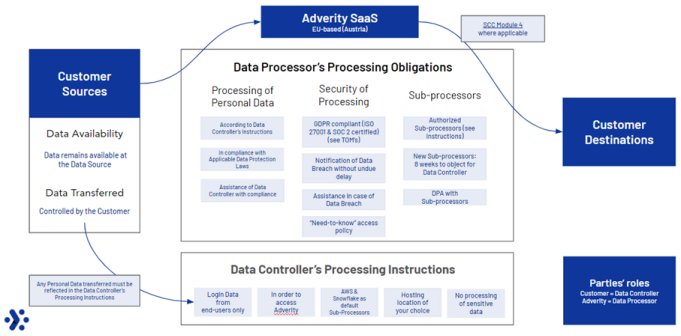
DATA PROCESSING AGREEMENT ("DPA")

THIS DATA PROCESSING AGREEMENT ("DPA") (in the version dated 2024-05-09) GOVERNS THE DATA PROCESSING OPERATIONS BETWEEN THE CUSTOMER ("DATA CONTROLLER") AND ADVERITY GMBH ("DATA PROCESSOR") WITH COMPANY REGISTRATION NUMBER 448481 g. BY ENTERING A COMMERCIAL AGREEMENT THAT REFERENCES THIS DPA, THE CUSTOMER AGREES TO THE TERMS AND CONDITIONS OF THIS DPA.

Table of Contents

Adverity GmbH's Data Processing Agreement as a Diagram



Infographic: Overview of this DPA (see enlarged version)

Data Controller's Processing Instructions

Back to top

Purposes	Provide access to and enable the use of the Data Processor's Software-as-a-Service (SaaS) and additional services as agreed between the Data Controller and the Data Processor.
Categories of Personal Data to be Processed by Default (*If the Data Controller intends to process other categories of Personal Data with the Data Processor's SaaS, the Data Controller must notify the Data Processor and an additional agreement must be concluded.)*	• Email Address • IP Address • Timestamps • Name (voluntarily)
Special Categories of Personal Data (If *the Data Controller instructs the Data Processor to process special categories of Personal Data on its behalf, the Data Controller shall ensure that all legal requirements for the processing of such special categories of Personal Data by the Data Processor (esp. those outlined in art. 9 (2) GDPR) are met at all times.*)	The Data Controller does not intend to and will not instruct the Data Processor to process any special categories of Personal Data.
Data Subjects by Default (*If the Data Controller intends to process Personal Data of additional Data Subjects with the Data Processor's SaaS, the Data Controller must notify the Data Processor and an additional agreement must be concluded.*)	• Users of the SaaS
Processing Operations	Collect, store, and process data to enable access to and use of the Data Processor's SaaS.
Sub-processor(s)	*Applicable in case of SaaS hosting by Data Processor:* • Amazon Web Services legal entity contracting with Austrian legal entities; or Google legal entity contracting with Austrian legal entities; or Microsoft Ireland Operations Ltd, (One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland). Purpose: Hosting infrastructure for servers and databases. If the Data Controller processes personal data of additional Data Subjects or additional Categories of Personal Data with the SaaS, the following Sub-processor is mutually agreed between the Parties: • Snowflake Computing Netherlands B.V. (Gustav Mahlerlaan 300, 1082 ME Amsterdam, The Netherlands). Purpose: Cloud-based data warehouse, that provides the infrastructure, storage and processing engine to power data reporting and analysis. *Applicable in case of SaaS hosting by Data Controller:* If the Data Controller processes personal data of additional Data Subjects or additional Categories of Personal Data with the SaaS, the following Sub-processor is mutually agreed between the Parties:

	• Snowflake Computing Netherlands B.V. (Gustav Mahlerlaan 300, 1082 ME Amsterdam, The Netherlands). Purpose: Cloud-based data warehouse, that provides the infrastructure, storage and processing engine to power data reporting and analysis.
Location of Processing Operations	*Applicable in case of SaaS hosting by Data Processor:* • If the Data Controller is based in the EU, the data will be hosted on servers located in a data center in the EU. • If the Data Controller is located outside the EU, the data might be hosted on servers inside or outside the EU. At the request of the Data Controller, the specific location will be communicated to the Data Controller. *Applicable in case of SaaS hosting by Data Controller:* • Hosting location is determined by the Data Controller.

Data Processor's Processing Obligations

Our DPA in plain language	*Talk legal to me - here is the full text of our DPA*

I. Background

Back to top

As provided under the Commercial Agreement, the Data Processor will process certain Personal Data while providing services to the Data Controller. This DPA will govern the Data Processor's data processing activities.	1. Within the scope and for the performance of the services defined in the Commercial Agreement, the Data Processor will process certain Personal Data on behalf of the Data Controller. 2. In addition to what may be provided in the Commercial Agreement, the following shall apply to the Data Processor's processing of Personal Data on behalf of the Data Controller to fulfill the requirements under Applicable Data Protection Legislation. Data Subjects, data categories as well as the extent, nature, and purpose of data processing are determined by the Commercial Agreement and "Data Controller's Processing Instructions" of this DPA.

II. Processing of Personal Data

Back to top

The Data Processor will comply with all relevant requirements under Applicable Data Protection Legislation while following the Data Controller's instructions, including assisting the Data Controller in meeting legal obligations, refraining from actions that could breach Applicable Data Protection	1. The Data Processor and any person acting under its authority (e.g. personnel, Sub-processors, and persons acting under the Sub-processor's authority) undertake to only process Personal Data as instructed in writing by the Data Controller (see the "Data Controller's Processing Instructions" above). The Data Processor shall only process Personal Data to the extent necessary to fulfill its obligations under this DPA

Legislation, and promptly notifying the Data Controller of any relevant communications or requests received from competent authorities.

The Parties will update the "Data Controller's Processing Instructions" to reflect any changes if needed.

or Applicable Data Protection Legislation.

2. If the services are altered during the term of the Commercial Agreement and such altered services involve new or amended processing of Personal Data, or if the Data Controller's instructions are otherwise changed or updated, the Data Controller shall instruct the Data Processor to update the "Data Controller's Processing Instructions" as appropriate before or at the latest in connection with the commencement of such processing or change.
3. The Data Processor shall comply with any Applicable Data Protection Legislation. The Data Processor shall keep itself updated on and comply with any changes in the Applicable Data Protection Legislation. The Data Processor shall make any necessary changes and amendments to this DPA required under Applicable Data Protection Legislation.
4. The Data Processor shall assist the Data Controller in fulfilling its legal obligations under Applicable Data Protection Legislation, including but not limited to:
   - protection of the rights of Data Subjects;
   - security of processing (Art. 32 GDPR);
   - notification of a personal data breach (Art. 33, 34 GDPR);
   - data protection impact assessment and the prior consultation (Art. 35, 36 GDPR); and
   - timely response to requests for exercising the Data Subject's rights to information regarding the processing of its Personal Data.

   The Data Processor shall not carry out or omit any act that would cause the Data Controller to be in breach of Applicable Data Protection Legislation.
5. The Data Processor shall immediately inform the Data Controller of a request, complaint, message, or any other communication received from a competent authority or any other third party regarding the processing of Personal Data covered by this DPA. The Data Processor may not in any way act on behalf of or as a representative of the Data Controller and may not, without prior instructions from the Data Controller, transfer or in any other way disclose Personal Data or any other information relating to the processing of Personal Data to any third party, unless the Data Processor is required to do so by law. The Data Processor shall assist the Data Controller in an appropriate manner to enable it to respond to such request, complaint, message, or other communication following Applicable Data Protection Legislation. In particular, the Data Processor shall not publish any submissions, notifications, communications, announcements, or press releases in the event of a breach of data protection as defined in Section XI. In the event the Data Processor, according to applicable laws and regulations, is required to disclose Personal Data that the Data Processor processes on behalf of the Data Controller, the Data Processor shall be obliged to inform the Data Controller thereof immediately unless prohibited by law.

III. Sub-processors

Back to top

The Data Controller authorizes the Data Processor to

1. The Data Controller authorizes the Data Processor to engage Sub-processors. All

engage Sub-processors to operate under the Data Controller's instructions. If the Data Processor intends to make changes to the current list outlined in the "Data Controller's Processing Instructions", it will notify the Data Controller in advance and the Data Controller can object within 8 weeks.

Sub-processors authorized by the Data Controller are acting under the authority and subject to direct instructions of the Data Controller. A list of the current Sub-processors is set out in the "Data Controller's Processing Instructions" for the purposes specified therein. The Data Processor shall notify the Data Controller in writing in advance of any changes, in particular before engaging other Sub-processors in which event the Data Processor shall without undue delay and no less than 8 weeks before transferring any Personal Data to a Sub-processor, inform the Data Controller in writing of the identity of such Sub-processor as well as the purpose for which it will be engaged.

2. The Data Controller at its discretion may object with good cause to any such changes within 8 weeks after the Data Processor's notice.

3. The Data Processor shall impose by written agreement, which includes an electronic form, on all Sub-processors processing Personal Data under this DPA (including inter alia its agents, intermediaries, and sub-contractors) the same obligations as apply to the Data Processor, in particular the obligations defined in Section III.1 (especially the procedure of notification to Data Controller and Data Controller's right to issue direct instructions to Sub-processors) and Section III.2 of this DPA.

IV. Transfer to Third Countries

Back to top

The Data Processor must obtain prior written consent from the Data Controller before transferring Personal Data outside the EU/EEA. Further, it will ensure compliance with Applicable Data Protection Legislation and incorporate the European Commission's Standard Contractual Clauses for adequate protection.

1. The location(s) of intended or actual processing of Personal Data is set out in the "Data Controller's Processing Instructions". The Data Processor must not transfer or otherwise directly or indirectly disclose Personal Data outside the European Economic Area ("EU/EEA") without the prior written consent of the Data Controller (which may be refused or granted at its discretion) and ensure that the level of protection of Data Subjects guaranteed by the GDPR and as outlined in this DPA is not undermined. Unless otherwise agreed between the Parties, adequate protection in the receiving country shall be secured through an agreement incorporating the European Commission's Standard Contractual Clauses.

2. If the Data Controller is located in a country, which is not a member of the EU/EEA and in case no Adequacy Decisions exist, the Standard Contractual Clauses (**Module 4: Processor-to-Controller**) shall apply to the transfer of Personal Data between the Data Processor and Data Controller and incorporated into this DPA by reference, and can be shared with the Data Controller upon request.

V. Security of Processing

Back to top

The Data Processor ensures the security of Personal Data through specified technical and organizational measures (see Appendix 1). Further, the Data Processor will notify the Data Controller of any security incidents, restrict access to authorized personnel bound by confidentiality obligations, and appoint a designated contact person for data

1. The Data Processor guarantees to implement and uphold appropriate technical and organizational measures according to the current state of the art to ensure an appropriate level of security for Personal Data and shall continuously review and improve the effectiveness of its security measures (See Appendix 1 hereunder). The Data Processor shall protect the Personal Data against destruction, modification, unlawful dissemination, or unlawful loss, alteration, or access. The Personal Data shall also be protected against all other forms of unlawful processing. With regard to the

protection matters without undue delay.

state of the art and the costs of implementation and taking into account the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, the technical and organizational measures to be implemented by the Data Processor shall include, as appropriate:

a. the pseudonymization and encryption of Personal Data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing Personal Data;
c. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

2. The Data Processor shall without undue delay notify the Data Controller of any Personal Data Breach after becoming aware of such incidents. The notification shall be in written form and shall at least:
   a. describe the nature of the Personal Data Breach including where possible, the categories and the approximate number of Data Subjects concerned and the categories and the approximate number of Personal Data records concerned;
   b. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
   c. describe the likely consequences of the Personal Data Breach;
   d. describe the measures taken or proposed to be taken by the Data Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects; and
   e. include any other information available to the Data Processor that the Data Controller is required to notify the Data Protection Authorities and/or the Data Subjects.

3. The Data Processor shall provide reasonable assistance requested by the Data Controller for the Data Controller to investigate the Personal Data Breach and notify the Data Protection Authorities and/or the Data Subjects as required by Applicable Data Protection Legislation.

4. The Data Processor shall at its own expense immediately take necessary measures to restore and/or reconstruct Personal Data that has been lost, damaged, destroyed, or corrupted as a result of any Personal Data Breach.

5. The Data Processor shall not disclose or otherwise make the Personal Data processed under this DPA available to any third party, without the Data Controller's prior written approval. For clarity, if the Data Processor is required by applicable laws and regulations to disclose Personal Data that the Data Processor processes on behalf of the Data Controller, Section II.5 shall apply.

6. The Data Processor shall ensure that access to Personal Data under this DPA is restricted to those of its personnel who directly require access to the Personal Data to fulfill the Data Processor's obligations under this DPA and the Commercial Agreement. The Data Processor shall ensure that such personnel (whether employees or others

engaged by the Data Processor):

a. has the necessary knowledge of and training in the Applicable Data Protection Legislation to perform the contracted services; and
b. is bound by a confidentiality obligation concerning the Personal Data to the same extent as the Data Processor under this DPA.

7. The Data Processor shall ensure that this confidentiality obligation extends beyond the termination of employment contracts, Sub-processor contracts, service contracts, or the termination of this DPA. This confidentiality obligation shall remain in force after the expiry or termination of the DPA.

8. The Data Processor appoints the following person as a contact point for data protection matters: Mr. Michael Pilz (dpo@adverity.com).

VI. Audit Rights

Back to top

The Data Processor grants the Data Controller (or an external auditor of the Data Controller's choice) the right to conduct audits on data protection and security to ensure compliance with this DPA and relevant data protection laws, and will provide all necessary information and assistance to demonstrate compliance.

1. The Data Processor shall allow the Data Controller or an external auditor appointed by the Data Controller to conduct audits, investigations, and inspections on data protection and/or data security ("audit") to ensure that the Data Processor or Sub-processors comply with the obligations under this DPA and Applicable Data Protection Legislation and that the Data Processor or Sub-processors have undertaken the required measures to ensure such compliance.

2. The Data Processor makes available all information necessary to demonstrate compliance with this DPA and Applicable Data Protection Legislation and assists the Data Controller in the performance of audits.

VII. Indemnification

Back to top

The Data Processor is responsible for indemnifying the Data Controller against claims from third parties arising from breaches caused by the Data Processor's intentional or grossly negligent actions under this DPA up to the fees paid by the Data Controller in the 12 months preceding the incident, except for willful intent, personal injuries, or death.

The Data Processor shall indemnify and hold harmless the Data Controller upon the Data Controller's first demand insofar as third parties (Data Subjects in particular) make claims against the Data Controller on the grounds of an infringement of their rights or of data protection law where such infringement is caused by actions of the Data Processor in intentional or grossly negligent violation of this DPA. The obligation to indemnify is – except in cases of willful intent or concerning personal injuries or death – capped with the amount of fees paid by the Data Controller in the 12 months immediately before the infringing incidence.

VIII. Term

Back to top

This DPA is in effect as long as the Data Processor handles Personal Data on behalf of the Data Controller.

1. This DPA shall remain in force as long as the Data Processor processes Personal Data on behalf of the Data Controller.

2. The Data Controller may terminate the Agreement without notice as a result of a breach of the obligations under this DPA by the Data Processor or one of its

Sub-processors.

IX. Notices

Back to top

In addition to other notice obligations provided hereunder, in case the Data Processor determines that any instruction to process data of the Data Controller violates Applicable Data Protection Legislation or substantial provisions of this DPA (including technical and organizational measures), it will immediately inform the Data Controller thereof.

X. Measures Upon Completion of Processing of Personal Data

Back to top

Personal data will be deleted or returned after contract fulfillment unless storage is required by law.

1. Upon expiration or termination of this DPA, the Data Processor shall delete or return all Personal Data (including any copies thereof) to the Data Controller, as instructed by the Data Controller, and shall ensure that any Sub-processors do the same unless otherwise required by applicable law. When returning the Personal Data, the Data Processor shall provide the Data Controller with all necessary assistance.

Written notice of measures taken can be provided to the Data Controller upon request.

2. Upon request by the Data Controller, the Data Processor shall provide written notice of the measures taken by itself or its Sub-processors concerning the deletion or return of the Personal Data upon the completion of the processing.

XI. Definitions

Back to top

For clarification purposes, the GDPR definitions of the relevant terms are used.

All terms used in this DPA are to be understood following the EU General Data Protection Regulation ((EU) 2016/679 "GDPR"), unless otherwise expressly agreed. The following terms and expressions in this DPA shall have the meaning set out below:

"Adequacy Decision" means a formal decision made by the EU Commission that recognizes that another country, territory, sector, or international organization provides an equivalent level of protection for personal data as the EU does.

"Applicable Data Protection Legislation" means any national or internationally binding data protection laws or regulations (including but not limited to the GDPR and the Austrian Data Protection Act ("DSG")) including any requirements, guidelines, and recommendations of the competent data protection authorities applicable at any time during the term of this DPA to, as the case may be, the Data Controller or the Data Processor.

"Data Controller" means the legal person which, alone or jointly with others, determines the purposes and means of the processing of Personal Data under this DPA.

"Data Processing Agreement" (or **"DPA"**) refers to this agreement which governs the data processing operations between the Data Controller and the Data Processor.

"Data Processor" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller under this DPA.

"EU/EEA" means European Union and/or European Economic Area.

"Personal Data" means any information relating to an identified or identifiable living, natural person ("Data Subject").

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

"Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means.

"Software-as-a-Service" (or **"SaaS"**) shall have the meaning as defined in Section I. of Adverity's Master Subscription Agreement.

"Standard Contractual Clauses" mean standard contractual clauses under the GDPR for data transfers from controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU/EEA (and not subject to the GDPR).

"Sub-processor" means any legal or natural person, including any agents and intermediaries, processing Personal Data on behalf of the Data Processor.

XII. Final Provisions

Back to top

In the event of a conflict with additional agreements, this DPA shall prevail regarding Personal Data processing, and be governed by Austrian law, with disputes subject to the jurisdiction of the Data Processor's registered seat; ineffective provisions will be replaced.

1. If the Data Controller and the Data Processor have entered into additional agreements in conflict with this DPA, the provisions of this DPA regarding the processing of Personal Data shall take priority, except where such provision is included in the Commercial Agreement to supplement this DPA. All other conflicting provisions shall be governed by the provisions of the Commercial Agreement.

2. This DPA is governed by the law of the Republic of Austria to the exclusion of the conflict law rules under private international law and the UN Convention on the International Sale of Goods. In the event of all disputes arising from a contract – including disputes about its existence or non-existence – the courts with subject-matter jurisdiction at the registered seat of the Data Processor shall be the exclusive forum.

3. The plain language descriptions in this DPA are for reference purposes only, and shall not in any way define, limit, or extend the scope of this DPA. If a provision or parts of a provision in this DPA is or becomes ineffective under applicable legislation, this will not affect the effectiveness and validity of the remaining provisions. The contracting parties will replace it with a provision which, in terms of content, is as close as possible to the ineffective provision.

Appendix 1 – Technical and Organizational Measures ("TOMs")

Back to top

The Data Processor confirms that the implemented technical and organizational measures provide an appropriate level of protection for the Data Controller's Personal Data considering the risks associated with the processing.

General Descriptions of Measures	*Description of Measures Implemented*
Physical Access and Environmental Control Suitable physical security and environmental controls are in place and designed to protect, control, and restrict physical access for systems and servers	Used hosting providers comply with: • information security standards such as with ISO 27018 and ISO 27001 and can provide certificates for evidence • AICPA SOC 2 standard and can provide reports for evidence
Logical Access Control (systems) Preventing data processing systems from being used without authorization	• Database security controls restrict access • Access rights are granted based on roles and need to know • Password policy based on established information security standards such as BSI and NIST • Automatic blocking of access (e.g. password, timeout) • Protocol of failed log-in attempts
Access Control (data) Ensuring that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that Personal Data cannot be read, copied, modified or removed without authorization	• Access rights are granted based on roles and need to know • Approval process for access rights • Periodical reviews of access rights • Signed confidentiality undertakings • Optional restricted to VPN (Virtual Privacy Networks) access only
Transmission Control Ensuring that Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to review and establish which bodies are to receive the Personal Data	• Encrypted transfer based on secure management of encryption keys and minimum requirements for encryption algorithm (e.g. AES 256) • Log files
Input Control Ensuring that it is possible to review and establish whether and by whom Personal Data have been input into data processing systems, modified, or removed	• Access rights granted based on roles and need to know • Approval process for access rights • Periodical reviews of access rights • Log files
Job Control Ensuring that the Personal Data is processed exclusively in accordance with the instructions	• Diligently selecting (Sub-)processors and other service providers • Documenting selection procedures (privacy and security policies, audit reports, certifications) • Backgrounds of service providers are checked, subsequent monitoring • Standardized policies and procedures (including clear segregation of responsibilities) • Documentation of instructions received from Data Controller • Signed confidentiality undertakings

Availability Control Ensuring that Personal Data is protected from accidental destruction and loss	Used hosting provider comply with: • Information security standards such as ISO 27018 and ISO 270001 and can provide certificates for evidence • AICPA SOC 2 standard and can provide reports for evidence Additional managed by Data Processor: • Backup procedures based on Business Impact Analysis • Disaster recovery plan • Routinely tests of disaster recovery plan
Separation Control Ensuring that data collected for different purposes can be processed separately	• Separate processing possibilities in the SaaS • Separation between productive and test data • Detailed management of access rights

Document Information

Document Owner: VP Legal & Compliance

Version: V6.0

Date of Version: 2024-05-09