DATA PROCESSING AGREEMENT ("DPA")

THIS DATA PROCESSING AGREEMENT ("DPA") (**in the version dated June 1, 2020**) 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, CUSTOMER AGREES TO THE TERMS AND CONDITIONS OF THIS DPA.

1. BACKGROUND

1. The Data Controller and the Data Processor have entered into the above-mentioned Commercial Agreement ("Agreement") under which the Data Processor shall provide certain services to the Data Controller. Within the scope and for the purpose of the performance of the services defined in the Agreement, the Data Processor will process beside other data potentially Personal Data on behalf of the Data Controller.

2. The Data Controller and the Data Processor have entered into this DPA in order to fulfill the requirement of a written agreement between a data controller and a data processor of Personal Data as set out in Applicable Data Protection Legislation. In addition to what may be set out in the Agreement, the following shall apply in relation to the Data Processor's processing of Personal Data on behalf of the Data Controller. Data Subjects, data categories as well as the extent, nature and purpose of data processing are determined by the Agreement, Appendix 1 to this DPA and the Data Controller's instructions.

2. DEFINITIONS

All terms used in this DPA are to be understood in accordance with 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:

"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 on, 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 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;
"Sub-processor" means any legal or natural person, including any agents and intermediaries, processing Personal Data on behalf of the Data Processor as set forth in Art 28 (2) and (4) GDPR and section 4.1 below;
"Personal Data" means any information relating to an identified or identifiable living, natural person ("data subject") as set forth in Art 4 (1) GDPR;
"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 as set forth in Art 4 (2) GDPR.

3. PROCESSING OF PERSONAL DATA

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 in accordance with documented instructions communicated by the Data Controller (Appendix 1). The Data Processor shall only process Personal Data to the extent necessary to fulfill its obligations under this DPA or Applicable Data Protection Legislation.
2. If the services are altered during the term of the 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 parties shall ensure that Appendix 1 is updated as appropriate before or at the latest in connection with the commencement of such processing or change.
3. When processing Personal Data under this DPA, the Data Processor shall comply with any and all Applicable Data Protection Legislation and applicable recommendations by competent Data Protection Authorities or other competent authorities and shall keep itself updated on and comply with any changes in such legislation and/or recommendations. The Data Processor shall accept to make any changes and amendments to this DPA that are 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 the Data Controller's obligation to comply with the rights of data subjects and in ensuring compliance with the Data Controller's obligations relating to the security of processing (Art. 32 GDPR), the notification of a Personal Data Breach (Art 33,

34 GDPR) and the Data Protection Impact Assessment and the prior consultation (Art 35, 36 GDPR), obligation to respond 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 any act, 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 him to respond to such a request, complaint, message or other communication in accordance with 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 6.3. 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.

4. SUB-PROCESSORS

1. The Data Controller authorizes the Data Processor to engage the Sub-processors. All 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 Appendix 1 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 at the latest 8 weeks prior to 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 own discretion may object 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 4.1 (in particular, procedure of notification to Data Controller and Data Controller's right to issue direct instructions to Sub-processors) and section 4.2 of this DPA.

5. TRANSFER TO THIRD COUNTRIES

1. The location(s) of intended or actual processing of Personal Data is set out in Appendix 1. The Data Processor must not transfer or otherwise directly or indirectly disclose Personal Data outside the European Economic Area without the prior written consent of the Data Controller (which may be refused or granted at its own discretion) and ensure that the level of protection of natural persons guaranteed by the GDPR and as set forth 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.

6. SECURITY OF PROCESSING

1. As set forth in Appendix 2, 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 the Personal Data and shall continuously review and improve the effectiveness of its security measures. 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. Having regard to the 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:

i. the pseudonymization and encryption of Personal Data;
ii. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing Personal Data;
iii. 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
iv. 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 accidental or unauthorized access or supposed access to Personal Data or any other actual or supposed, threatened or potential security incidents (personal data breach) after becoming aware of such incidents. The notification shall be in written form and shall at least:
   i. describe the nature of the Personal Data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;
   ii. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
   iii. describe the likely consequences of the personal data breach;
   iv. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;
   v. include any other information available to the Data Processor which the Data Controller is required to notify the Data Protection Authorities and/or the data subjects.
3. The Data Processor will furthermore provide reasonable assistance requested by the Data Controller for the Data Controller to investigate the personal data breach and notify it to the Data Protection Authorities and/or the data subjects as required by Applicable Data Protection Legislation.
4. In addition, 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 the personal data breach.
5. The Data Processor undertakes to 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. This section 6.5 shall not apply 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, in which case what is set out in section 3.5 shall apply.
6. The Data Processor undertakes to ensure that access to Personal Data under this DPA is restricted to those of its personnel who directly require access to the Personal Data in order to fulfill the Data Processor's obligations in accordance with this DPA and the Agreement. The Data Processor shall ensure that such personnel (whether employees or others engaged by the Data Processor) (i) has the necessary knowledge of and training in the Applicable Data Protection Legislation to perform the contracted services; and (ii) is bound by a confidentiality obligation concerning the Personal Data to the same extent as the Data Processor in accordance with this DPA.
7. The Data Processor requires all of its personnel (employees and Sub-processors) authorized to process Personal Data not to process Personal Data for any other purpose, except on instructions from the Data Controller or unless required by applicable law. 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 responsible for data protection matters: Mr. Michael Pilz (dpo@adverity.com).

7. AUDIT RIGHTS

1. The Data Processor shall allow the Data Controller or an external auditor mandated by the Data Controller to conduct audits, investigations and inspections on data protection and/or data security ("audit") in order

to ensure that the Data Processor or Sub-processors are able to 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.

8. INDEMNIFICATION

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 Controller on the grounds of an infringement of their personal rights or of data protection law where such infringement is caused by actions of the Processor in intentional or gross negligent violation of this DPA. The obligation to indemnify is – except in cases of willful intent or in relation to personal injuries or death – capped with the amount of fees paid by the Controller in the 12 months immediately before the infringing incidence.

9. TERM

1. The term of this DPA follows the above-mentioned Agreements.
2. In case of a termination of the Agreement, this DPA shall remain in force as long as the Data Processor processes Personal Data for the Data Controller.
3. 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.

10. NOTICES

1. Any notice or other communication to be provided by one party to the other party under this DPA, shall be provided in accordance with the notices provision of the Agreement.
2. 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.

11. MEASURES UPON COMPLETION OF PROCESSING OF PERSONAL DATA

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

12. FINAL PROVISIONS

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. 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.

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 by a provision which, in terms of content, is as close as possible to the ineffective provision.

Appendix 1 - Data Processing Instructions

Purposes Specify all purposes for which the Personal Data will be processed by the Data Processor.	Marketing data reporting and analytics.
Categories of Data Specify the different types of Personal Data that will be processed by the Data Processor	*The following Personal Data is processed by default. If the Data Controller intends to process other categories of Personal Data with the Application Services of the Data Processor, the latter must be notified hereof, and an additional agreement must be concluded.* ● Email Address ● Name (on a voluntary basis)
Data Subjects Specify the categories of data subjects whose personal data will be processed by the Data Processor.	*The following categories of data subjects are affected by the data processing operations by default. If the Data Controller intends to process Personal Data of other categories of data subjects with the Application Services of the Data Processor, the latter must be notified hereof, and an additional agreement must be concluded.* ● Users of the Application Services
Processing Operations Specify all processing activities to be conducted by the Data Processor	Collect, harmonize, store, and analyze data.
Sub-processor(s) Specify the Sub-processors engaged by the Data Processor (if any) and the purposes for which the personal data is processed by such Sub-processor	*Applicable in case of Application Services hosting by Data Processor:* 1. Amazon Web Services EMEA SARL (5 rue Plaetis, L-2338 Luxembourg); or Google Ireland Limited (Gordon House, Barrow Street, Dublin 4, Ireland); or Microsoft Ireland Operations Ltd, (One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland). Purpose: Hosting infrastructure for server and databases. 2. Adverity Inc. (980 6th Ave, 3rd Floor, New York, NY 10018, USA) Purpose: Support of internal business operations. *Applicable in case of Application Services hosting by Data Controller:* 1. Adverity Inc. (980 6th Ave, 3rd Floor, New York, NY 10018, USA) Purpose: Support of internal business operations.
Location of Processing Operations Specify all locations where the Personal Data will be processed by the Data Processor and any Sub-processor (if applicable)	*Applicable in case of Application Services 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 Application Services hosting by Data Controller:* ● Austria and Data Processing Service Center of Data Controller.

Appendix 2 - Technical and Organizational Measures ("TOMs")

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 Description of Measures	Description of Measures Implemented
Access Control (premises) Preventing unauthorized persons from gaining access to data processing systems	• Used hosting provider complies: • with ISO 27018 which is based on ISO 27000 • Access control systems (smart cards, biometric control) • Security personnel at entrances (backgrounds checked) • Right to access generally limited • List of authorized people (manager approval required) • Surveillance systems (alarm system, door prop alarm, motion detectors, 24x7 CCTV) • Visitor logbook (time and purpose of entry, time of exit)
Access Control (systems) Preventing data processing systems from being used without authorization	• Database security controls restrict access • Access rights based on roles and need to know • Password policy • 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 based on roles and need to know • Approval process for access rights; periodical reviews and audits • Signed confidentiality undertakings • Optional restricted to Office IPs
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 (HTTPS, SSL, SSH; RSA, 4096-bit keys) • 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 based on roles and need to know • Approval process for 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	• Redundant uninterruptible power supply (UPS)

Ensuring that Personal Data is protected from accidental destruction and loss	● Air-conditioning, temperature and humidity controls (monitored 24x7) ● Disaster-proof housing (smoke detection, fire alarm, fire suppression, water detection, raised flooring, protection against severe weather conditions, pest repellent system) ● Electrical equipment monitored and logged, 24x7 support ● Daily backup procedures ● Disaster recovery plan ● Routinely test-running data recovery
<u>Separation Control</u> Ensuring that data collected for different purposes can be processed separately	● Separate processing possibilities in the Application Services for HR data, production data, supplier data, customer data ● Separation between productive and test data ● Detailed management of access rights

Document Information	
Document Owner	Head of Legal
Version	V2.0
Date of Version	06/01/20