TERMS OF USE (“TOU”)

THESE TERMS OF USE (**in the version dated September 02, 2022**) GOVERN THE USE BY ANY PERSON OR ENTITY OF THE APPLICATION SERVICES (AS DEFINED BELOW) PROVIDED BY ADVERITY GMBH WITH COMPANY REGISTRATION NUMBER 448481 g.

PLEASE READ THESE TERMS CAREFULLY BEFORE USING THE APPLICATION SERVICES!

1. SCOPE OF APPLICATION

a. Adverity exclusively provides its Application Services to entrepreneurs. The User represents and warrants that they act as an entrepreneur and is not considered as a consumer. The User further represents and warrants that neither minors, consumers nor other unauthorized third-parties use the Application Services within their sphere of responsibility.
b. Any terms and conditions of the User, that deviate from the TOU shall be ineffective, even if they claim (exclusive) validity.
c. Adverity is entitled to amend the TOU at any time at its discretion following section 16.
d. By agreeing to the TOU and/or by using the Application Services, the User agrees to be legally bound by all terms, conditions, and notices contained or referenced in these TOU as well as by the Data Processing Agreement. If the User disagrees with any of the above-mentioned terms, they may not use the Application Services. For the sake of clarity, each User expressly agrees to be bound by these TOU.

2. DEFINITIONS

“**Account**” means the account for the Platform, created by each user to access the Application Services. The Account is strictly limited to the use of one user.
“**Adverity**” means Adverity GmbH, an Austrian company whose registered business address is Rathausstrasse 1/2nd Floor, 1010 Vienna, registered at Handelsgericht Wien with the company registration number 448481g and all its Affiliates.
“**Administrator**” means a natural person who is designated by the User’s company to administer the Application Services on behalf of the User’s company, including granting access to the Application Services as well as enabling features and functions on the Platform, that could incur additional costs.
“**Affiliate**” means an affiliated entity that is directly or indirectly, through one or more intermediaries, controlled by, or is under common control with, another person or entity. The term “controlled” means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through the ownership of voting stock, by contract, or otherwise.
“**Applicable Law**” means all laws, regulations, and legal obligations which are applicable in the Republic of Austria, including the provisions on the competent court of jurisdiction.
“**Application Services**” means the products and services offered by Adverity, which User orders based on a commercial agreement, a proof-of-concept agreement, or a similar agreement and are made available online by Adverity via a password-protected user login.
“**Beta Services**” means any products or services created or provided by Adverity that are not generally available to Adverity’s users.
“**Confidential Information**” shall have the meaning outlined in section 10.
“**Effective Date**” means the date on which an agreement about the provision of the Application Services is concluded between the Parties or, at the latest, the date on which User started using the Application Services.

"**Feedback**" means any materials, including but not limited to comments, suggestions, ideas, or other information provided by the User to Adverity.
"**Malicious Code**" means viruses, worms, time bombs, trojan horses, and other harmful or malicious code, files, scripts, agents, or programs.
"**Party**" and "**Parties**" means Adverity and/or the User concerning their business relationship.
"**Platform**" refers to a specific URL, provided by Adverity, where the Application Services are operating.
"**Subscription**" means the provision of the Application Services from Adverity to User via the Platform.
"**Subscription Term**" means the agreed period for which Adverity makes available the Application Services to the User.
"**TOU**" means these Terms of Use, which are deemed to be accepted by using the Application Services.
"**User**" means anyone who uses the Application Services.
"**User Data**" means all electronic data or information submitted by the User to the Application Services.
"**User Guide**" means online help, training, how-to documents, and explanatory materials that assist the User in using the Application Services (as such materials may be updated from time to time), accessible via log-in to the Application Services or otherwise as made available by Adverity.

3. ACCOUNT REGISTRATION

To use the Application Services, an Account will be provisioned to the User and the latter must represent and warrant:

a. to provide Adverity with accurate, up-to-date, and complete information, which is required to set up an account;
b. to keep any logins, passwords, or other credentials in connection with the Application Services secret;
c. to maintain and promptly update any information the User provides to Adverity; and
d. to notify Adverity immediately of any unauthorized use of this information or any other breach of security within their sphere of responsibility by sending an email to support@adverity.com.

4. USE OF APPLICATION SERVICES

a. The User shall:
    i. be responsible for their compliance with the TOU, the Applicable Law as well as for the accuracy, quality, and legality of the User Data and of how the User acquires the User Data. The User represents and warrants that the User Data will not infringe any copyright, patent, trade secret, or other proprietary right held by any third party;
    ii. use all reasonable efforts to prevent unauthorized access to, or use of, the Application Services, and notify Adverity promptly of any such unauthorized access or use;
    iii. use the Application Services only following the User Guide and the Applicable Law; and
    iv. use each registration and each Account exclusively by themselves. The joint use of one Account by several people or the transfer of the Account to a third party, either against payment or for free, is strictly forbidden.
b. The User shall not:
    i. make the Application Services available to anyone else;
    ii. sell, resell, rent, or lease the Application Services or the right to use them;
    iii. use the Application Services to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party rights;
    iv. use the Application Services to store or transmit Malicious Code;

v. interfere with or disrupt the integrity or performance of the Application Services or third-party data contained therein;
vi. attempt to gain unauthorized access to the Application Services or their related systems or networks; or
vii. use the Application Services beyond the scope permitted in writing.

c. In the event, the User breaches any provision of the TOU Adverity may, in addition to any other right which Adverity might have under the Applicable Law, suspend the User's access to the Application Services.

5. THIRD-PARTY SERVICES

a. The Application Services allow the User to gather data from multiple third-party data sources and services, including various third-party websites. The third-party services from which the data can be gathered are selected by Adverity at its sole discretion and Adverity reserves the right to select, discontinue and change such available sources at any time. Adverity assumes no liability whatsoever for the data or other content collected from third-party services.
b. The User is solely responsible for ascertaining that they have the right to use the third-party services for gathering and processing any such data by using the Application Services, and the User must obtain any such consents and authorizations as may be needed from time to time concerning such data or other content and their processing.
c. The Application Services may be used as an add-on to various third-party services and software. Adverity does not assume any liability for such third-party services or software, the User is exclusively responsible for obtaining any necessary licenses or consents needed for their use. The User must familiarize themselves with the applicable terms and conditions, including any restrictions on use, concerning any such third-party services the User agrees to comply with such third-party terms and conditions in addition to the TOU.
d. Furthermore, the Application Services may contain links to websites and content of third parties as a service to those interested in this information. Adverity does not monitor, endorse, or adopt, or have any control over, any third-party content. Adverity undertakes no responsibility to update or review any third-party content and can make no guarantee as to its accuracy or completeness. Additionally, if the User follows a link or otherwise navigates away from the Application Services, they need to be aware that the TOU will no longer govern. The User should review the applicable terms and policies, including privacy and data gathering practices, of any third-party content or service provider to which they navigate from the Application Services. The User accesses and uses third-party content at their own risk.
e. The Application Services may contain advertisements and promotions from third parties. The User's business dealings or correspondence with, or participation in promotions of, advertisers other than Adverity, and any terms, conditions, warranties, or representations associated with such dealings, are solely between the User and such third party.

6. MODIFICATIONS TO THE APPLICATION SERVICES

a. Adverity reserves the right to modify, discontinue, and restrict, temporarily or permanently, all or part of the Applications Services at its sole discretion. Neither Adverity nor its suppliers will be liable to the User or any third party for any modification, discontinuance, or restriction of the Application Services.
b. If Adverity ceases the Application Services, it shall – at its sole discretion – and as the User's exclusive remedy;

i. permit the User to continue the use of the Application Services until the end of the Subscription Term; or
ii. terminate the Subscription of the User before the end of the Subscription Term and refund them any pre-paid Subscription Fee on a prorated basis.

c. From time to time, Adverity may invite the User to try, at no additional charge, Beta Services. Any Beta Services will be designated as beta, pilot, limited release, developer preview, non-production, or by a description of similar import. Beta Services are provided for evaluation purposes and not for production use, are not supported, may contain bugs or errors, are subject to change in Adverity's sole discretion, and may be subject to additional terms. The User shall immediately inform Adverity of any bugs or errors experienced, and otherwise, provide its feedback to, and cooperate with, Adverity on Beta Services as reasonably requested by Adverity. Beta Services are provided "as is" with no express or implied warranty and Adverity disclaims all liability for Beta Services. Adverity may discontinue Beta Services at any time in Adverity's sole discretion and may never make them generally available.

7. USER'S FEEDBACK

The User grants Adverity a nonexclusive, royalty-free, perpetual, irrevocable, and fully sublicensable right to use their feedback for any purpose without compensation or attribution to the User.

8. PROPRIETARY RIGHTS

a. Adverity reserves all rights, title, and interest in and to the Application Services, including all related intellectual property rights. No rights are granted to User hereunder other than as expressly set forth herein.
b. User shall not:
   i. modify, copy, or create derivative works based on the Application Services;
   ii. reverse engineer the Application Services; or
   iii. access the Application Services to
      - build a competitive product or service, or
      - copy any ideas, features, functions, or graphics of the Application Services.
c. As between User and Adverity, User shall own all User Data, including all reports, statistics, and other data to the extent generated solely from User Data, and all intellectual property rights therein.
d. Adverity shall own all rights, title, and interest, including all intellectual property rights, in and to any improvements to the Application Services or any new programs, upgrades, modifications, or enhancements developed by Adverity in connection with rendering the Application Services to User, even when refinements and improvements result from User's request or suggestion. In the case that the intellectual property rights of such refinements and improvements are not automatically transferred to Adverity under the TOU or otherwise, User hereby transfers and assigns (and, if applicable, shall cause its Affiliates to transfer and assign) to Adverity all rights, title, and interest which User or its Affiliates may have in or to such refinements and improvements.
e. The User agrees that Adverity may disclose the relationship between the User and Adverity as well as the User's name and logo on Adverity's website and in promotional materials.

9. INDEMNIFICATION

a. Adverity shall defend User against any claim, demand, suit, or proceeding made or brought against User by a third party alleging that the use of the Application Services as permitted hereunder infringes or misappropriate the intellectual property rights of a third party (a "Claim Against User"), and shall indemnify User for any damages, attorneys' fees and other costs finally awarded against User as a result of, and for amounts paid by User under a court-approved settlement of, a Claim Against User; provided that User:
   i. promptly gives Adverity written notice of the Claim Against User;
   ii. gives Adverity sole control of the defense or settlement of the Claim Against User (provided that Adverity may not settle any Claim Against User unless the settlement unconditionally releases Customer of all liability); and
   iii. provides to Adverity reasonable assistance, at Adverity's expense. If Adverity receives information regarding an infringement, misappropriation, or another claim, Adverity may in Adverity's discretion, and at no cost to User
      - modify the Application Services, so that they no longer infringe,
      - misappropriate, or give rise to any other claim;
      - obtain a license for User's continued use of the subject Application Services following the TOU; or
      - terminate the User's Subscription for such Application Services upon 30 days written notice and refund to User any prepaid fees covering the remainder of the term of the terminated Subscription.

b. Adverity shall have no obligation to indemnify User to the extent any Claim Against User arises from User's breach of these Terms.

c. The User shall defend Adverity against any claim, demand, suit, or proceeding made or brought against Adverity by a third party alleging that the User Data or the use of the Application Services by the User is in breach of these Terms, infringe or misappropriate the property rights of a third party or violates Applicable Law and shall indemnify Adverity for any damages, attorneys' fees, and other costs finally awarded against Adverity as a result of, or for any amounts paid by Adverity under a court-approved settlement of a claim against Adverity, provided that Adverity:
   i. promptly gives the User written notice of the claim against Adverity;
   ii. gives the User sole control of the defense or settlement of the claim against Adverity (provided that the User may not settle any claim against Adverity unless the settlement unconditionally releases Adverity of all liability); and
   iii. provides to the User all reasonable assistance, at the User's expense.

10. CONFIDENTIAL INFORMATION

a. "Confidential Information" means (a) any technical and business information relating to proprietary ideas, patentable ideas and/or trade secrets, existing and/or contemplated products and services, research and development, production, costs, profit and margin information, finances and financial projections, clients, marketing, and current or future business plans and models, regardless of whether such information is designated as "Confidential Information" at the time of its disclosure; (b) any product information of Adverity's Application Services as well as data transferred via the Application Services; (c) in addition to the above, Confidential Information shall also include, and the Parties shall have a duty to protect other confidential and/or sensitive information which is (I) disclosed as such in writing and marked as confidential (or with other similar designation) at the time of disclosure; and/or (II) disclosed in any other manner and identified as confidential at the time of disclosure and which is summarized and designated as

confidential in a written memorandum delivered within 30 days after the disclosure; and (d) excludes any information that is (I) is in possession of a Party prior to its receipt from the other Party; (II) is or becomes publicly known without a breach of this section 10.; (III) is developed independently by the other Party; or (IV) is received from another source who can disclose it lawfully and without an obligation to keep it confidential.

b. The Parties shall only use the Confidential Information for the Purpose and shall not disclose the Confidential Information to third parties. Either Party may disclose the other Party's Confidential Information if required by law as long as the other Party will be informed promptly by written notice (to the extent permitted by law) of the requirement before the disclosure and assistance will be provided to the other Party in obtaining an order protecting the information from public disclosure. Neither party shall reverse engineer, disassemble, or decompile any prototypes, software, samples, or other tangible objects that embody the Confidential Information.
c. The Parties acknowledge that the Confidential Information is a valuable, special, and unique asset for each Party which shall be protected with the highest standard of care. Therefore, the Parties agree that they shall not disclose, utilize, employ, exploit or in any other manner use the Confidential Information disclosed by the other Party for any other reason than the Purpose. The Parties shall limit disclosure of Confidential Information within their organization to those directors, officers, partners, contractors, and/or employees having a need to know and shall not disclose Confidential Information to any third party without the prior written consent of the other Party. Before the disclosure, each Party must ensure that the recipients are required to protect the Confidential Information on terms as protective as this section 10. and accept responsibility for each recipient's use of Confidential Information. Upon request, the Parties shall provide each other with a complete and updated list of all such recipients. The Parties shall take reasonable measures to protect the secrecy of and avoid disclosure and/or unauthorized use of the Confidential Information. A Party shall promptly notify the other Party of any actual or suspected unauthorized use or disclosure of the Confidential Information.
d. If a Party discloses Confidential Information in violation of this section 10., the Party in breach shall notify the other Party in writing of such disclosure immediately upon discovery of the violation and no later than 5 business days after such disclosure.
e. Neither Party shall be obliged to disclose or provide any Confidential Information to the other Party. Nothing in this section 10. shall obligate the Parties to purchase any service, goods, or intangibles from the other Party or to proceed with any transaction between them or contemplated by this section 10.
f. ALL CONFIDENTIAL INFORMATION IS PROVIDED "AS IS." THE PARTIES MAKE NO WARRANTIES, EXPRESS, IMPLIED, OR OTHERWISE, REGARDING THE ACCURACY, COMPLETENESS, OR PERFORMANCE OF ITS CONFIDENTIAL INFORMATION. EACH PARTY REPRESENTS AND WARRANTS THAT IT HAS THE RIGHT TO DISCLOSE ALL CONFIDENTIAL INFORMATION PROVIDED TO THE OTHER PARTY. THE PARTIES SHALL INDEMNIFY AND DEFEND EACH OTHER FROM ALL THIRD-PARTY CLAIMS RESULTING FROM THE NEGLIGENT OR WRONGFUL DISCLOSURE OF A THIRD PARTY'S CONFIDENTIAL INFORMATION.
g. All documents and other tangible objects containing or representing Confidential Information and all copies of them shall be and remain the property of the disclosing Party and shall be promptly returned to this Party or destroyed (with proof of such destruction), each within 14 days of the written request or upon the termination of the Parties' business relationship.

h. Nothing in this section 10. is intended to grant any rights in or to the Confidential Information, including without limitation, under any patent, copyright, or another intellectual property right of the other Party.
i. Each Party acknowledges that any violation or threatened violation of this section 10. may cause irreparable injury to the other Party, entitling the other Party to seek injunctive relief in addition to all legal remedies.

11. DATA PROTECTION

The User agrees to be legally bound by all terms, conditions and notices contained or referenced in the Data Processing Agreement (find below), which forms an integral part of the TOU.

12. AGGREGATED ANONYMOUS DATA

a. Notwithstanding anything to the contrary herein, the User consents that Adverity may obtain and aggregate technical and other data about the User's use of the Application Services.
b. In addition to the aforementioned, Adverity may obtain and aggregate marketing metrics data as statistical averages for benchmarking purposes if the Administrator consents thereto by enabling certain features and functions within the Platform in relation to benchmarking.
c. Such aggregated data is anonymous and non-personally identifiable concerning the User. Adverity may use it to analyze, improve, support, and operate the Application Services, and for commercial distribution of benchmarking data and industry reports. In that case, Adverity will not identify the User as a source of any aggregated anonymous data.

13. DISCLAIMER & LIMITATION OF LIABILITY

a. THE APPLICATION SERVICES ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. ADVERITY MAKES NO REPRESENTATIONS, WARRANTIES, TERMS, CONDITIONS, OR STATEMENTS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE REGARDING ANY MATTER, INCLUDING THE MERCHANTABILITY, SUITABILITY, OR FITNESS FOR A PARTICULAR USE OR PURPOSE, OR THAT THE OPERATIONS OF THE APPLICATION SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE.
b. ANY (OPTIMIZATION) RECOMMENDATIONS, SUGGESTIONS, OR FORECASTS CREATED BY THE APPLICATION SERVICES AND BASED ON THE DATA PROVIDED BY THE USER ARE NOT GUARANTEED TO BE CORRECT. ADVERITY MAKES NO WARRANTIES OR REPRESENTATIONS, EXPRESS, IMPLIED, OR OTHERWISE REGARDING THE ACCURACY, COMPLETENESS, OR PERFORMANCE OF THE PROVIDED INFORMATION. USER ACKNOWLEDGES THAT ADVERITY CANNOT BE HELD LIABLE AT ANY TIME FOR ANY LOSSES DUE TO DECISIONS OR TRANSACTIONS MADE BASED ON THIS INFORMATION.
c. EXCEPT FOR BODILY INJURY OF A PERSON, ADVERITY, ITS SUPPLIERS, OFFICERS, AFFILIATES, REPRESENTATIVES, CONTRACTORS, AND EMPLOYEES SHALL NOT BE RESPONSIBLE OR LIABLE CONCERNING ANY SUBJECT MATTER OF THIS TOU UNDER ANY CONTRACT, NEGLIGENCE STRICT LIABILITY, OR OTHER THEORY FOR AN ERROR OR INTERRUPTION OF THE USE OF FOR LOSS OR INACCURACY OR CORRUPTION OF DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE SERVICES OR TECHNOLOGY OR LOSS OF BUSINESS, FOR ANY INDIRECT, EXEMPLARY, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR FOR ANY MATTER BEYOND ADVERITY'S REASONABLE CONTROL. ADVERITY'S TOTAL LIABILITY SHALL BE LIMITED TO THE SUM

OF ALL FEES PAID BY THE USER TO ADVERITY IN 12 MONTHS PRECEDING THE DAMAGING EVENT.

d. ADVERITY SHALL NOT BE LIABLE FOR ANY LOSS OF, OR DAMAGE TO, DATA OR PROGRAMS TO THE EXTENT THAT SUCH LOSS OR DAMAGE WOULD HAVE BEEN AVOIDED OR MITIGATED BY ADEQUATE PREVENTATIVE MEASURES OF THE USER.

14. ASSIGNMENT

The Subscription is not assignable, transferable, or sublicensable by the User except with Adverity's prior written consent. Adverity may transfer and assign any of its rights and obligations under the TOU without consent to an Affiliate.

15. SEVERABILITY CLAUSE

Should one or more provisions of the TOU be or become invalid, the remaining clauses of the TOU shall not be affected. The Parties shall replace the invalid provision with a replacement provision that would have been agreed by the Parties according to their original economic intentions. This principle shall also apply in the case of any unintentional contractual gaps.

16. AMENDMENTS TO THE TERMS OF USE

a. Adverity is entitled to amend the TOU from time to time for any reason by giving the User notice via email or through the Application Service Platform.

b. If the User does not agree to the amendments, Adverity shall, at its sole decision and as the User's exclusive remedy;

   i. permit the User to continue the use of the Application Services according to the prior version of the Terms until the end of the then-current Subscription Term; or

   ii. terminate the Subscription of the User before the end of the Subscription Term and refund them any pre-paid Subscription Fee on a prorated basis.

c. Upon any amendment to these Terms, the User may be required to actively consent to the updated Terms by clicking a consent button within the Platform. The continued use of the Application Services, after the amendments of the Terms become effective, constitutes the User's acceptance of the amendments.

17. GOVERNING LAW

These Terms shall be governed exclusively by the laws which are applicable in the Republic of Austria (without regard to its conflict of law rules and the United Nations Convention on Contracts for the International Sale of Goods ["CISG"]). Exclusive legal venue for all disputes under or in connection with the Terms shall be with the courts of Vienna, Austria, having subject matter and territorial jurisdiction.

18. SURVIVING PROVISIONS

The following provisions shall survive even after the Subscription has ended: USER'S FEEDBACK; PROPRIETARY RIGHTS; INDEMNIFICATION; CONFIDENTIAL INFORMATION; DATA PROTECTION; AGGREGATED ANONYMOUS DATA; DISCLAIMER & LIMITATION OF LIABILITY; AMENDMENTS TO THE TERMS OF USE; GOVERNING LAW.

DATA PROCESSING AGREEMENT ("DPA")

THIS DATA PROCESSING AGREEMENT ("DPA") **(in the version dated September 02, 2022**) 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.

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 performance of the services defined in the Agreement, the Data Processor will process besides other data potentially Personal Data on behalf of the Data Controller.
2. The Data Controller and the Data Processor have entered into this DPA 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 concerning 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 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:

"**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 who, 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, a natural person ("data subject") as set forth in Art 4 (1) GDPR;

"**Processing**" means any operation or set of operations that 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 a 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, the 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

The location(s) of the 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; the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of systems and services processing Personal Data;
    ii. 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
    iii. 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 another 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 Data 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 Data Processor in intentional or grossly 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 number 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 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, except where such provision is included in the Commercial Agreement for the purpose of supplementing 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. 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 that, in terms of content, is as close as possible to the ineffective provision.

Appendix 1 to the DPA - Data Processing Instructions

Purposes Specify all purposes for which the Personal Data will be processed by the Data Processor.	Provide access to Data Processor's marketing data reporting and analytics Application Services.
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 ● IP Address ● Timestamps ● Name (on a voluntary basis)
Special categories of Personal Data Specify the different special categories of Personal Data that will be processed by the Data Processor	The Controller does not intend to and will not instruct the Processor to process any special categories of Personal Data. In the event that 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 set forth in art. 9 (2) GDPR) are met at all times.
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, store, and process data to enable access to the Data Processor's Application Services.
Sub-processor(s) Specify the Sub-processors engaged by the Data Processor (if any) and the	*Applicable in case of Application Services hosting by Data Processor:*

purposes for which the personal data is processed by such Sub-processor	1. 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. 2. Snowflake Computing Netherlands B.V. (Gustav Mahlerlaan 300, 1082 ME Amsterdam, The Netherlands) Purpose: Database. 3. Adverity Inc. (75 Rockefeller Plaza, Suite 22B, New York, NY 10019, USA). Purpose: Support internal business operations. 4. Diva-e NEXT GmbH (St. Martin Straße 72, 81541 Munich, Germany). Purpose: Provision of onboarding services. *Applicable in case of Application Services hosting by Data Controller:* 1. Snowflake Computing Netherlands B.V. (Gustav Mahlerlaan 300, 1082 ME Amsterdam, The Netherlands) Purpose: Database. 2. Adverity Inc. (75 Rockefeller Plaza, Suite 22B, New York, NY 10019, USA). Purpose: Support internal business operations. 3. Diva-e NEXT GmbH (St. Martin Straße 72, 81541 Munich, Germany). Purpose: Provision of onboarding services.
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:*

	• 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.

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 has been	• Access rights based on roles and need to know • Approval process for access rights • Log files

input into data processing systems, modified, or removed	
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 the data controller • Signed confidentiality undertakings
Availability Control Ensuring that Personal Data is protected from accidental destruction and loss	• Redundant uninterruptible power supply (UPS) • 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
Separation Control 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: VP Legal & Compliance

Version: V3.4

Date of Version: 2022-09-02