TERMS OF USE

These are the Terms of Use ("Terms") of Adverity GmbH ("Adverity"), an Austrian company whose registered business address is Rathausstrasse 1/2nd Floor, 1010 Vienna, registered at Handelsgericht Wien with the company registration number 448481g.

PLEASE READ THESE TERMS CAREFULLY BEFORE USING THE APPLICATION SERVICES.

1. SCOPE OF APPLICATION

a. These Terms are effective as of **February 3, 2020** between Adverity and the user ("User") and shall be applicable to all services ("Application Services") provided by Adverity via the Application Service platform ("Platform").

b. Adverity exclusively provides its Application Services to entrepreneurs. The User represents and warrants that they act as an entrepreneur according to the meaning of the Austrian Commercial Code ("Unternehmensgesetzbuch" or "UGB") and is not considered as consumer according to the Austrian Consumer Protection Law ("Konsumentenschutzgesetz" or "KSchG"). The User further represents and warrants that neither minors, consumers nor other unauthorized third parties use the Application Services within their sphere of responsibility.

c. Any terms and conditions of the User that deviate from the Terms shall be ineffective, even if they claim (exclusive) validity.

d. Adverity is entitled to amend the Terms at any time at its discretion in accordance with clause 18.

e. By agreeing to the Terms or by using the Application Services, the User agrees to be legally bound by all terms, conditions and notices contained or referenced in these Terms as well as by the Data Processing Agreement, Adverity's Privacy Notice and Adverity's Data Protection Guidelines. 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 Terms.

2. DEFINITIONS

a. **"Account"** refers to the account for the Platform, created by each User in order to access the Application Services. The Account is strictly limited to the use by one User.

b. **“Adverity”** refers to 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.

c. **“Affiliate”** refers to an affiliated entity pursuant to Section 189a No. 8 and/or an associated entity pursuant to Section 189a No. 9 Austrian Commercial Code.

d. **“Applicable Law”** refers to all laws, regulations and legal obligations which are applicable in the Republic of Austria, including the provisions on the competent court of jurisdiction.

e. **“Application Services”** refers to the software-as-a-service products “Adverity Datatap”, “Adverity Insights” and “Adverity Presense” offered by Adverity, which are made available to the User online via the Platform. The Application Services enable the User to collect, harmonize, store especially marketing related data from various sources and allow to analyze, report and visualize this data.

f. **“Beta Services”** refers to products or services created or provided by Adverity that are not generally available to Adverity’s users.

g. **“Confidential Information”** refers to all information disclosed by a Party (“Disclosing Party”) to the other Party (“Receiving Party”), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Confidential Information also includes 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, customers, 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. Adverity’s Confidential Information shall include the Application Services, the Platform and all related information.

h. **“Feedback”** refers to any materials, including but not limited to comments, suggestions, ideas, or other information provided by the User to Adverity.

i. **“Malicious Code”** refers to viruses, worms, time bombs, trojan horses and other harmful or malicious code, files, scripts, agents or programs.

j. **“Party”** and **“Parties”** refers to Adverity and/or the User with respect to their legal relationship.

k. **“Platform”** refers to a specific URL, provided by Adverty, where the Application Services are operating.

l. **“Subscription”** refers to the provision of the Application Services from Adverity to the User via the Platform.

m. **“Subscription Fee”** refers to the payable fee paid by the User to Adverity.

n. **“Subscription Term”** refers to the agreed period for which Adverity makes available the Application Services to the User.

o. **“Terms”** refers to these Terms of Use, which are accepted by the User prior to first use by clicking on the consent checkbox on the Platform.

p. **“User”** refers to anyone who uses the Application Services from Adverity on the basis of these Terms.

q. **“User Data”** refers to the data provided by the User to Adverity in order to process this data via the Application Services.

r. **“User Guide”** refers to online help, training, how-to documents and explanatory materials that assist the User in using the Application Services, accessible via the Platform or otherwise as made available by Adverity.

3. ACCOUNT REGISTRATION

a. In order to use the Application Services, a user account (“Account”) must be provisioned and the User must represent and warrant:

   i. to provide Adverity with accurate, uptodate and complete information, which is required to set up an account;

   ii. to keep any logins, passwords, or other credentials in connection with the Application Services secret;

   iii. to maintain and promptly update any information the User provides to Adverity; and

   iv. 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 these Terms, the Applicable Law as well as for the accuracy, quality and legality of the User Data and of the means by which the User acquires the User Data. The User Data shall not infringe on 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;

iii. use the Application Services only in accordance with the User Guide and in accordance with Applicable Law; and

iv. use each account registration exclusively for one user. The joint use of an account by several people or the transfer of an account to a third party, either against payment or for free, is forbidden.

b. The User shall not:

i. make the Application Services available to anyone other than their employees and contractors who are authorized by the User to use the Application Services;

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 permitted scope or in a manner that violates the Applicable Law.

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

d. If the User wants to enable any third party to access their account for the Application Services a separate contract needs to be concluded between Adverity and the User in order to create an “External Business User Account”. Such a contract can be requested by sending an email to support@adverity.com.

e. In consideration of the above-mentioned, the User still can use the data provisioning features of Adverity Datatap or the dashboard sharing and export functionalities of Adverity Insights.

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 in relation to 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 licences or consents needed for their use. The User must familiarise themselves with the applicable terms and conditions, including any restrictions on use, in relation to any such third-party services the User agrees to comply with such third-party terms and conditions in addition to these Terms.

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 navigate away from the Application Services they need to be aware that these Terms 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 or its suppliers will be liable to the User or to 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 clearly 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 any and 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. FEES AND PAYMENT

a. The Application Services are made available to the User against payment of the Subscription Fee.

b. Invoices are issued according to the Parties agreement, starting with the first day of the Subscription Term. The Subscription Fee is to be paid net within 30 days of receipt of the invoice.

c. Overdue Subscription Fees accrue late interest at the statutory rate.

d. If any amount owed by the User is 30 days or more overdue, Adverity may, without limiting Adverity’s other rights and remedies, accelerate the User’s unpaid fee obligations so that all such obligations become immediately due and payable, and suspend provision of the Application Services until such amounts are paid in full. Adverity will give the User at least 7 days prior notice that the User’s account is overdue before suspending the Application Services.

e. The Subscription Fee does not include any taxes, levies, duties or similar governmental assessments of any nature, including but not limited to value added, sales, use or withholding taxes, collected by any local, state, provincial, federal or foreign jurisdiction.

8. 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.

9. PROPRIETARY RIGHTS

a. Adverity reserves all rights, title and interest in and to the Application Services, including all related copyrights, trademarks and intellectual property rights. No proprietary rights are granted to the User hereunder other than as expressly set forth herein.

b. The 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 in order to

        I. build a competing product or service, or

        II. copy any ideas, features, functions, or graphics of the Application Services.

c. The User shall own all User Data, including all reports, statistics, and other data to the extent generated solely from the User Data, and all property rights therein.The User hereby grants to Adverity a non-exclusive, worldwide, royalty-free right to use, copy, store, transmit, modify, create derivative works of and display the User Data solely to the extent necessary to provide the Application Service to the User.

d. Adverity owns all rights, title and interest, including all copyrights, trademarks and 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 the User, even when refinements and improvements result from User's request or suggestion. In the case that the copyrights, trademarks and intellectual property rights of such refinements and improvements are not automatically transferred to Adverity by virtue of the Terms, the Applicable Law or otherwise, the User hereby transfers and assigns (and, if applicable, shall cause its Affiliates to transfer and assign) to Adverity all rights, title, and interest which the 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.

10. CONFIDENTIAL INFORMATION

a. As used herein, "Confidential Information" means all information disclosed by a party ("Disclosing Party") to the other party ("Receiving Party"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure.

b. The Parties agree that all Confidential Information of the Disclosing Party constitutes property according to clause 9 of the latter.

c. Confidential Information shall not include any information that is in possession of the Receiving Party prior to receipt from the Disclosing Party, is or becomes publicly known, otherwise than as a consequence of a breach of this clause, is developed independently by the Receiving Party, is disclosed by the Receiving Party to satisfy a legal demand by a competent court of law or governmental body or by any applicable regulatory authority or security exchange; or is disclosed to a third party pursuant to a written authorization from the Disclosing Party.

d. The Receiving Party shall

   i. use the same degree of care that it uses to protect the confidentiality of its own Confidential Information (but in no event less than reasonable care)

   ii. will not disclose, utilize, employ, exploit or in any other manner use the Confidential Information disclosed by the Disclosing Party for any reason or purpose other than to fulfil its obligations arising out of cooperation between the Parties;

iii. except as otherwise authorized by the Disclosing Party in writing, limit access to Confidential Information of the Disclosing Party to those of its and its Affiliates' employees, contractors, and agents who need such access for purposes consistent with the use of the Application Services and who have signed agreements with the Receiving Party containing protections no less stringent than those herein. Neither party shall disclose the Terms or any subsequent Agreement between the Parties to any third party, other than its Affiliates and their legal counsel and accountants, without the other Party's prior written consent; and

e. The Receiving Party may disclose Confidential Information of the Disclosing Party if it is compelled by law to do so, provided the Receiving Party gives the Disclosing Party prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure. If the Receiving Party is compelled by law to disclose the Disclosing Party's Confidential Information as part of a civil proceeding to which the Disclosing Party is a party, and the Disclosing Party is not contesting the disclosure, the Disclosing Party will reimburse the Receiving Party for its reasonable cost of compiling and providing secure access to such Confidential Information.

f. The obligations of each Party shall continue, even if the Subscription Term has ended.

g. In the event that the Receiving Party discloses Confidential Information in violation of these Terms the Disclosing Party must be promptly notified of such disclosure in writing after such disclosure.

h. The Parties each expressly agree that due to the unique nature of the Disclosing Party's Confidential Information, monetary damages may be inadequate to compensate the Disclosing Party for any breach by the Receiving Party of this clause. Accordingly, the Parties each agree and acknowledge that any such violation or threatened violation shall cause irreparable injury to the Disclosing Party and that, in addition to any other remedies that may be available, in law, in equity or otherwise, the Disclosing Party shall be entitled to seek injunctive relief against the threatened breach or the continuation of any such breach by the Receiving Party.

i. Each Party represents and warrants that it has the right to disclose all Confidential Information that it discloses to the other Party. Each Party will indemnify and defend the other from all third-party claims resulting from the negligent or wrongful disclosure by the indemnifying party of a third-party's confidential information.

j. Upon termination of the Subscription the Disclosing Party may request within 7 days in writing that any Confidential Information disclosed to the Receiving Party be returned or deleted.

11. AGGREGATED ANONYMOUS DATA

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. Such aggregated anonymous data is non-personally identifiable with respect to the User Adverity may use it to analyze, improve, support and operate the Application Services, and for its distribution in general benchmarking data and industry reports. In that case Adverity will not identify the User as source of any aggregated anonymous data.

12. DATA PROTECTION

The User agrees to be legally bound by all terms, conditions and notices contained or referenced in the Data Processing Agreement, Adverity's Privacy Notice and Adverity's Data Protection Guidelines.

13. INDEMNIFICATION BY ADVERITY

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:

a. promptly gives Adverity written notice of the Claim Against User;
b. 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
c. provides to Adverity reasonable assistance, at Adverity's expense. If Adverity receives information regarding an infringement, misappropriation, or other claim, Adverity may in Adverity's discretion, and at no cost to User

i. modify the Application Services, so that they no longer infringe, misappropriate, or give rise to any other claim, without breaching Adverity's warranties under Section VII.2 above;

ii. obtain a license for User’s continued use of the subject Application Services in accordance with this Agreement; or

iii. terminate User’s subscriptions 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 subscriptions.

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

14. INDEMNIFICATION BY USER

a. 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 are 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.

15. WARRANTY DISCLAIMER

The Application Services are provided on an “as is” and “as available” basis. Adverity and its suppliers and licensors expressly disclaim all warranties of any kind, whether expressed or implied, including but not limited to the implied warranty of merchantability, fitness for a particular purpose, title, and non-infringement. Adverity does not warrant uninterrupted use or operation of the Application Services or the User’s access to the Platform.

16. LIMITATION OF LIABILITY

a. Notwithstanding anything to the contrary, except for bodily injury of a person, Adverity, its suppliers, officers, affiliates, representatives, contractors and employees shall not be responsible or liable with respect to any subject matter of these Terms of Use 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.

b. Adverity's total liability shall be limited to the sum of all Subscriptions Fees paid by the User to Adverity in a 12 month period preceding the damaging event.

c. 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.

17. TERMINATION AND RENEWAL

a. The Subscription to the Application Services remains in effect for the Subscription Term agreed by the Parties.

b. The Subscription shall automatically renew for additional periods equal to the expiring Subscription Term or one year (whichever is higher), unless either Party gives the other notice of non-renewal at least 90 days before the end of the relevant Subscription Term. The per-unit pricing during any such renewal term shall be the same as that during the prior term unless Adverity has given the User written notice of a pricing increase at least 90 days before the end of the last possible termination date for the renewal term, in which case, if the User does not terminate, the pricing increase shall be effective upon renewal and thereafter.

c. Either Party may terminate the Subscription for cause at any time upon 30 days' written notice to the other Party

   i. of a material breach, if such breach remains uncured at the expiration of such period; or

   ii. if the assets of the other Party become the subject of a petition in bankruptcy or in any other similar proceeding.

d. Upon any termination for cause by the User, Adverity shall refund the User any prepaid fees covering the remainder of the Subscription Term after the effective date of termination. Upon any termination for cause by Adverity, the User shall pay any unpaid fees covering the remainder of the Subscription Term after the effective date of termination. In no event shall any termination relieve the User of the obligation to pay any Subscription Fee payable to Adverity for the period prior to the effective date of termination.

e. For a period of 7 days after termination of the Subscription, the User Data remains stored in the Application Services. At the conclusion of the 7-day period, Adverity shall delete the User Data from the Application Services and shall destroy any corresponding documents under its control, except to the extent that Adverity is bound by the Applicable Law to continue storing such User Data.

18. SURVIVING PROVISIONS

The following provision shall survive even after the Subscription has ended.

AGGREGATED ANONYMOUS DATA; AMENDMENTS TO THE TERMS OF USE; CONFIDENTIAL INFORMATION; DATA PROTECTION; INDEMNIFICATION BY USER; FEES AND PAYMENT; LIMITATION OF LIABILITY; PROPRIETARY RIGHTS; SURVIVING PROVISIONS; USER'S FEEDBACK; WARRANTY DISCLAIMER:

19. AMENDMENTS TO THE TERMS OF USE

a. Adverity is entitled to amend the Terms 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.

20. 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 to 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.

21. ASSIGNMENT

The Subscription and therefore the Terms are not assignable, transferable or sublicensable by User except with Adverity's prior written consent. Adverity may transfer and assign any of its rights and obligations under these Terms without consent to an affiliated company.

22. SEVERABILITY CLAUSE

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

DATA PROCESSING AGREEMENT (“DPA”)

entered into between the User (“Data Controller”) and Adverity (“Data Processor”). This DPA constitutes an integral part of the Terms agreed between the Data Controller and Data Processor.

1. BACKGROUND

1. The Data Controller and Data Processor have agreed the above-mentioned Terms 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 Terms, the Data Processor will process beside other data potentially Personal Data on behalf of the Data Controller.
2. The Data Controller and 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 Terms, 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 Terms, 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 General Data Protection Regulation [“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 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(s)”: 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 agreed Subscription Term 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 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 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

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 Terms. 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 the 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 data protection law where such infringement is caused by the 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 Terms.
2. In case of a termination of the Terms, 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 Terms 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 in writing.
2. In case the Data Processor determines that any instructions to process data of the Data Controller violates Applicable Data Protection Laws 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 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.
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 part 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

x Email address

x Name

x Any other personal data which the Data Controller may process through the Application Services of the Data Processor

Data subjects

Specify the categories of data subjects whose personal data will be Processed by the Data Processor.

x Customers

x Prospects

x 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

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.

Location of processing operations

Specify all locations where the personal data will be processed by the Data Processor and any sub-processor (if applicable)

The data will be hosted according to the Data Controller’s demand on available servers provided by the chosen Sub-processor.

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 taking into account 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, 24×7 CCTV)
- Visitor log book (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

Ensuring that personal data is protected from accidental destruction and loss

- Redundant uninterruptible power supply (UPS)

- Air-conditioning, temperature and humidity controls (monitored 24×7)
- 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, 24×7 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