# TERMS OF USE ("TOU")

THESE TERMS OF USE (in the version dated January 23, 2026) GOVERN THE USE BY ANY PERSON OR ENTITY OF THE ADVERITY SAAS (AS DEFINED BELOW) PROVIDED BY ADVERITY GMBH WITH COMPANY REGISTRATION NUMBER 448481

PLEASE READ THESE TERMS CAREFULLY BEFORE USING THE ADVERITY SAAS!

The plain language descriptions in these TOU are for reference purposes only, and shall not in any way define, limit, or extend the scope of the TOU.

---

## Table of Contents


### Users' Matters

I. SaaS Description and Account Registration
II. Users' Rights and Responsibilities

### Legal Matters

III. Intellectual Property Rights
IV. Disclaimer and Limitation of Liability
V. Indemnification
VI. Data Protection
VII. Mutual Confidentiality Clauses
VIII. Miscellaneous
IX. Definitions


---

# Users' Matters

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

## I. SaaS Description and Account Registration

Back to top

| | |
|---|---|
| *Adverity's Integrated Data Platform is a SaaS solution that streamlines data integration and governance processes.* | **1. SaaS Description**<br><br>Adverity's Integrated Data Platform is a SaaS (Software-as-a-Service) data Platform for connecting, managing, and using data at scale. Adverity automates complex data integration and governance processes, before transferring data to the destination selected by the User.<br><br>Adverity only processes the following personal data by default on behalf of the Customer : login credentials (name, email, IP-address and time-stamp) belonging to the User(s) of Adverity. Adverity`s DPA stipulates the mutual rights and obligations with regards to data protection. |
| *To access the SaaS, a User Account is provisioned based on the agreement. Each User must provide accurate information, safeguard credentials, keep details updated, and report security breaches to Adverity.* | **2. Account Registration**<br><br>To use the SaaS, a User Account will be provisioned to the User based on the respective greement.<br><br>Each User represents and warrants:<br><br>a. to provide Adverity with accurate, up-to-date, and complete information, which is required to set up a User-Account;<br>b. to keep any logins, passwords, or other credentials in connection with the SaaS secret;<br>c. to maintain and promptly update any information the User provides to Adverity; and,<br>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. |

## II. Users' Rights and Responsibilities

Back to top

| | |
|---|---|
| *The User is responsible for ensuring compliance with the TOU, applicable laws, and the accuracy and legality of their data, must protect the SaaS from unauthorized use, follow the documentation and legal guidelines, and refrain from sharing or misusing their User-Account, with violations leading to suspension of access.* | **1. User's Responsibilities**<br><br>a. The User shall:<br>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;<br>ii. use all reasonable efforts to prevent unauthorized access to, or use of, the SaaS, and notify Adverity promptly of any such unauthorized access or use;<br>iii. Use the SaaS only following the Documentation and the Applicable Law; and |

iv. Use each registration and each User-Account exclusively by themselves. The joint use of one User-Account by several people or the transfer of the User-Account to a third party, either against payment or for free, is strictly forbidden.

b. The User shall not:
   i. make the SaaS available to anyone else;
   ii. sell, resell, rent, or lease the SaaS or the right to use them;
   iii. use the SaaS 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 SaaS to store or transmit Malicious Code;
   v. interfere with or disrupt the integrity or performance of the SaaS or third-party data contained therein;
   vi. attempt to gain unauthorized access to the SaaS or their related systems or networks;
   vii. use the SaaS beyond the scope permitted in writing;
   viii. modify, copy, or create derivative works based on the SaaS; ii. reverse engineer the SaaS; or
   ix. access the SaaS to:
      1. build a competitive product or service, or
      2. copy any ideas, features, functions, or graphics of the SaaS.

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 SaaS.

*The SaaS allows users to gather data from third-party sources selected by Adverity, which assumes no liability for such data or third-party services, while the user is responsible for obtaining necessary permissions, complying with third-party terms, and using the SaaS at their own risk, including any third-party content, ads, or promotions.*

**2. Third-Party Services**

a. The SaaS allows 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 SaaS, 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 SaaS 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 SaaS 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 SaaS, 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 SaaS. The User accesses and uses third-party content at their own risk.

e. The SaaS 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.

*Adverity reserves the right to modify, discontinue, or restrict the SaaS at its discretion, with no liability to the user or third parties, and may offer Beta Services for evaluation, which are provided "as is" with no warranty and may be discontinued or altered at any time.*

**3. Modifications of the SaaS**

a. Adverity reserves the right to modify, discontinue, and restrict, temporarily or permanently, all or part of the SaaS 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 SaaS.

b. If Adverity ceases the SaaS, Adverityt shall – at its sole discretion – and as the User's exclusive remedy;
   i. permit the User to continue the use of the SaaS until the end of the Subscription Term; or
   ii. terminate the User's right to use the SaaS before the end of the Subscription Term.

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.

# Legal Matters

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

## III. Intellectual Property Rights

Back to top

*The SaaS and any improvements to the SaaS belong to Adverity.*

**1. Adverity IP**

Adverity reserves all rights, title, and interest in and to the SaaS, including all related intellectual property rights. In addition, Adverity owns all rights, title, and interest, including all intellectual property rights, in and to any improvements to the SaaS or any new programs, upgrades, modifications or enhancements developed by Adverity in

| | |
|---|---|
| | connection with rendering the SaaS to User, even when refinements and improvements result from User's request or suggestion.<br>Except for the limited rights expressly granted herein, Adverity does not transfer to User any proprietary right or interest in the Services. All rights not expressly granted to User in the Agreement are reserved to Adverity. |
| *User Data and reports generated from User Data belong to User.* | **2. User IP**<br><br>As between Adverity and the User, User owns User Data, including all reports, statistics, and other data to the extent generated solely from User Data, and all intellectual property rights therein. Notwithstanding the foregoing, Adverity shall have the right to collect and use User Data in relation to the provision of the Services to User, including in order to improve and enhance the Services. |
| *User's Feedback can be used by Adverity without restriction.* | **3. User's Feedback**<br><br>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. |
| *The User consents that Adverity may collect and aggregate anonymous, non-personally identifiable data on SaaS usage and marketing metrics for analysis, improvement, benchmarking, and commercial distribution.* | **4. Aggregated Anonymous Data**<br><br>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 SaaS.<br>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 SaaS in relation to benchmarking.<br>c. Such aggregated data is anonymous and non-personally identifiable concerning the User. Adverity may use it to analyze, improve, support, and operate the SaaS, 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. |

## IV. Disclaimer and Limitation of Liability

Back to top

| | |
|---|---|
| *Adverity provides the SaaS on an "as is" and "as available" basis without warranties or guarantees of uninterrupted, error-free performance, accuracy, or suitability, disclaims liability for indirect or consequential damages, limits total liability to fees paid in the preceding 12 months, and is not responsible for data loss that could have been mitigated by the User's preventive measures.* | a. THE SAAS 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.<br>b. ANY (OPTIMIZATION) RECOMMENDATIONS, SUGGESTIONS, OR FORECASTS CREATED BY THE SAAS 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.<br>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 OR, WHERE RELEVANT, CUSTOMER TO ADVERITY WITH REGARDS TO THE RESPECTIVE SERVICE / FEATURE IN 12 MONTHS PRECEDING THE DAMAGING EVENT, IF ANY.

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.
e. IN ANY CASE, ANY LIABILITY UNDER THIS TOU SHALL BE LIMITED TO THE MAXIMUM EXTEND PERMITTED BY APPLICABLE LAW.

## V. Indemnification

Back to top

*Adverity indemnifies User for infringement or misappropriation of a third party's IP by the SaaS.*

**1. 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 SaaS as permitted hereunder infringes or misappropriates 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 User 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 SaaS, so that they no longer infringe, misappropriate, or give rise to any other claim;
    ii. obtain a license for User's continued use of the SaaS under this TOU; or
    iii. terminate User's right to use the SaaS upon 30 days written notice.

Adverity shall have no obligation to indemnify User to the extent any Claim Against User arises from User's breach of the terms of this TOU.

*User indemnifies Adverity for infringement of third-party IP or violation of the law resulting out of the use of User Data or misuse of the SaaS.*

**2. Indemnification by User**

User shall defend Adverity against any claim, demand, suit or proceeding made or brought against Adverity by a third party alleging that User Data, or User's use of the Services in breach of this TOU, infringes or misappropriates the intellectual property rights of a third party or violates applicable law (a "Claim Against Adverity"), 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:

a. promptly gives User written notice of the Claim Against Adverity;

b. gives User sole control of the defense or settlement of the Claim Against Adverity (provided that User may not settle any Claim Against Adverity unless the settlement unconditionally releases Adverity of all liability); and
c. provide to User all reasonable assistance, at User's expense.

## VI. Data Protection

Back to top

The User acknowledges and agrees that, where a Customer acts as a data controller under applicable data protection laws, User is solely responsible for ensuring that it has obtained all necessary rights, authorizations, and legal bases to instruct Adverity to process any personal data on its behalf. The User represents and warrants that any such processing by Adverity in connection with the provision of the services governed by this TOU does not and will not violate any applicable laws, regulations, or third-party rights.

*The Data Processing Agreement below applies where applicable under applicable data protection laws.*

Where required under applicable data protection laws, or where necessary to supplement an existing Data Processing Agreement between the Customer and Adverity in relation to any services governed by these TOU, the Data Processing Agreement available as an Appendix 1 shall be deemed concluded between the Customer and Adverity. The User further confirms that it has all necessary rights and authorization to bind the Customer to the terms of the Data Processing Agreement, should such agreement or any part of it be required under applicable data protection laws.

The User shall indemnify, defend, and hold harmless Adverity from and against any claims, damages, or liabilities arising from its failure to comply with this obligation.

## VII. Mutual Confidentiality Clauses

Back to top

*This confidentiality section includes a customary definition of Confidential Information, encompassing typical exceptions.*

**1. Definition of Confidential Information**

a. "Confidential Information" means all information disclosed by a Party ("Disclosing Party") to the other Party ("Receiving Party") that reasonably should be understood to be confidential. User Confidential Information shall include User Data; Adverity Confidential Information shall include the SaaS; and Confidential Information of each Party shall include the terms and conditions of this TOU.
b. Confidential Information also includes:
    i. technical and business information of any kind, regardless of whether such information is designated as "Confidential Information" at the time of its disclosure;
    ii. any SaaS or product-related information of Adverity Platforms as well as data transferred via the Platforms.
c. Confidential Information shall not include any information that:
    i. is in possession of the Receiving Party prior to receipt from the Disclosing Party;
    ii. is or becomes publicly known, otherwise than as a consequence of a breach of this TOU;
    iii. is developed independently by the Receiving Party;
    iv. 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
    v. is disclosed to a third party pursuant to written authorization from the Disclosing Party.

*Both parties commit to safeguarding the Confidential Information of the other Party as*

**2. Protection of Confidential Information**

| | | |
|---|---|---|
| *if it were their own, restricting access to a need-to-know basis and to achieve the purpose of this TOU.* | The Receiving Party:<br>a. shall 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);<br>b. 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 fulfill its (pre-contractual) obligations arising out of cooperation between the Parties;<br>c. shall only use the Confidential Information for the purpose of using or providing the SaaS in accordance with this TOU and shall not disclose the Confidential Information to third parties.<br><br>The obligations under this Section of each of the Parties shall continue, even if the contractual relationship between them has ended, without any restriction. | |
| *Compelled disclosure is explicitly excluded.* | **3. Compelled Disclosure**<br><br>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. | |
| | **4. Unintentional Disclosure and Remedies**<br><br>a. If the Receiving Party discloses Confidential Information in violation of the Terms of this TOU, the Disclosing Party shall be promptly notified of such disclosure in writing after such disclosure.<br>b. 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 its covenants and agreements outlined in this Section. 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 of this Section or the continuation of any such breach by the Receiving Party.<br>c. Each Party 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. | |
| *At the request of the Disclosing Party, the Receiving Party will either return or destroy the Confidential Information.* | **5. Request for Return**<br><br>The Disclosing Party may request in writing at any time that any Confidential Information disclosed to the Receiving Party be returned with a written statement to the effect that upon such return it has not retained in its possession or under its control, either directly or indirectly, any Confidential Information. The Receiving Party shall comply with any such request within thirty (30) days of receipt of such request. If the Receiving Party objects to such request for return, the Confidential Information shall be destroyed upon request by the Disclosing Party. In such case, the Receiving | |

Party shall provide the Disclosing Party with a written statement under oath certifying that the respective Confidential Information has been destroyed.

## VIII. Miscellaneous

Back to top

### 1. Assignment

Your use 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.

### 2. 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.

*Governing law will be Austrian law with forum in Vienna, Austria .*

### 3. Governing Law and Jurisdiction

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.

### 4. 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 SaaS.
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 SaaS according to the prior version of the Terms until the end of the then-current Subscription Term; or
    ii. terminate User's right to use the SaaS before the end of the Subscription Term.
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 SaaS. The continued use of the SaaS, after the amendments of the Terms become effective, constitutes the User's acceptance of the amendments.

### 5. Surviving Provisions

The following provisions shall survive even after User's right to use the SaaS has ended: INTELLECTUAL PROPERTY RIGHTS; INDEMNIFICATION; MUTUAL CONFIDENTIALITY CLAUSES; DATA PROTECTION; DISCLAIMER & LIMITATION OF LIABILITY; AMENDMENTS TO THE TERMS OF USE; GOVERNING LAW.

### 6. Conflict between plain language and full text

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

## IX. Definitions

Back to top

**"Administrator"** means a natural person who is designated by the User's company to administer the SaaS on behalf of the User's company, including granting access to the SaaS 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.

**"Commercial Agreement"** means the documents for placing orders for Adverity SaaS that are entered between Adverity and its Customer (likely to be User's company), including addenda and supplements thereto.

**"Customer"** means an entity that has entered into an agreement (including, but not limited to Commercial Agreement) with Adverity and has authorized the User to use its Subscription to the Adverity SaaS.

**"Documentation"** means online help, training, how-to documents, and explanatory materials that assist Users in using the SaaS (as such materials may be updated from time to time), accessible via log-in to the SaaS or otherwise as made available by Adverity.

**"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 SaaS is operating.

**"SaaS"** means Adverity Integrated Data Platform, a SaaS data Platform for connecting, managing, and using data at scale, which Adverity makes available to Users online via a password-protected Customer login.

**"Subscription"** means the provision of the SaaS from Adverity to Adverity's Customer via the Platform and under which the User is entitled to use the Platform.

**"Subscription Term"** means the agreed period for which Adverity makes available the SaaS to Adverity's Customer and for which the User is entitled to use the Platform.

**"User"** means anyone who is authorized to use the SaaS.

**"User-Account"** means the account for the Platform, created by each User to access the SaaS. The User-Account is strictly limited to the use by one User.

**"User Data"** means all electronic data or information submitted by the User to the SaaS.

# Appendix 1: DATA PROCESSING AGREEMENT ("DPA")

WHERE REQUIRED UNDER APPLICABLE DATA PROTECTION LAWS, OR WHERE NECESSARY TO SUPPLEMENT AN EXISTING DATA PROCESSING AGREEMENT BETWEEN THE CUSTOMER AND ADVERITY IN RELATION TO ANY SERVICES GOVERNED BY THE TOU, THIS DATA PROCESSING AGREEMENT ("DPA") (in the version dated

2026-01-23) GOVERNS THE DATA PROCESSING OPERATIONS BETWEEN THE CUSTOMER ("DATA CONTROLLER") AND ADVERITY GMBH ("DATA PROCESSOR") WITH COMPANY REGISTRATION NUMBER 448481 g.

THE USER CONFIRMS THAT IT HAS ALL NECESSARY RIGHTS AND AUTHORIZATION TO BIND THE CUSTOMER TO THE TERMS OF THE DATA PROCESSING AGREEMENT.

---

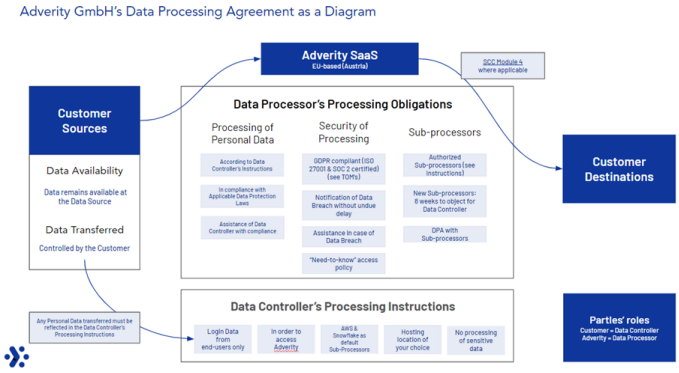
## Table of Contents


**Data Controller's Processing Instructions**

**Data Processor's Processing Obligations**

I. Background
II. Processing of Personal Data
III. Sub-processors
IV. Transfer to Third Countries
V. Security of Processing
VI. Audit Rights
VII. Indemnification
VIII. Term
IX. Notices
X. Measures Upon Completion of Processing Personal Data
XI. Definitions
XII. Final provisions

**Appendix I - Technical and Organizational Measures (TOMs)**


Infographic: Overview of this DPA (see enlarged version)

---

# Data Controller's Processing Instructions

Back to top

| | |
|---|---|
| **Purposes** | Provide access to and enable the use of the Data Processor's Software-as-a-Service (SaaS) and additional services as agreed between the Data Controller and the Data Processor. |
| **Categories of Personal Data to be Processed by Default**<br>(*If the Data Controller intends to process other categories of Personal Data with the Data Processor's SaaS, the Data Controller must notify the Data Processor and an additional agreement must be concluded.)* | • Email Address<br>• IP Address<br>• Timestamps<br>• Name (voluntarily)<br>• Additional Personal Data categories processed in the SaaS, if any. |
| **Special Categories of Personal Data**<br>(If *the Data Controller instructs the Data Processor to process special categories of Personal Data on its behalf, the Data Controller shall ensure that all legal requirements for the processing of such special categories of Personal Data by the Data Processor (esp. those outlined in art. 9 (2) GDPR) are met at all times.*) | The Data Controller does not intend to and will not instruct the Data Processor to process any special categories of Personal Data. |
| **Data Subjects by Default**<br>(*If the Data Controller intends to process Personal Data of additional Data Subjects with the Data Processor's SaaS, the Data Controller must notify the Data Processor and an additional agreement must be concluded.*) | • Users of the SaaS<br>• Additional Data Subjects categories processed in the SaaS, if any. |
| **Processing Operations** | Collect, store, and process data to enable access to and use of the Data Processor's SaaS. |
| **Sub-processor(s)** | |

| Sub-processor | Purpose |
|---|---|
| Amazon Web Services legal entity contracting with Austrian legal entities<br><br>Google legal entity contracting with Austrian legal entities<br><br>Microsoft Ireland Operations Ltd (One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland) | Hosting Infrastructure (applicable if SaaS hosting by Data Processor)<br><br>Enabling Adverity's AI functionalities (applicable if the Data Controller processes personal data in Adverity's SaaS and shares it with the AI functionalities) |
| Snowflake Computing BV (Gustav Mahlerlaan 300, 1082 ME Amsterdam, The Netherlands) | Cloud-based data warehouse for reporting and analysis (applicable if the Data Controller processes personal data in Adverity's SaaS) |
| OpenAI Ireland Ltd (1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland) | Enabling Adverity's AI functionalities (applicable if the Data Controller processes personal data in Adverity's SaaS and shares it with the AI functionalities) |

| | | |
|---|---|---|
| | | |
| **Location of Processing Operations** | *Applicable in case of SaaS hosting by Data Processor:*<br>• If the Data Controller is based in the EU, the data will be hosted on servers located in a data center in the EU.<br>• If the Data Controller is located outside the EU, the data might be hosted on servers inside or outside the EU.<br>At the request of the Data Controller, the specific location will be communicated to the Data Controller.<br>*Applicable in case of SaaS hosting by Data Controller:*<br>• Hosting location is determined by the Data Controller. | |

## Data Processor's Processing Obligations

| *Our DPA in plain language* | *Talk legal to me - here is the full text of our DPA* |
|---|---|
| **I. Background** | Back to top |
| *As provided under the TOU, the Data Processor will process certain Personal Data while providing services to the Data Controller. This DPA will govern the Data Processor's data processing activities.* | 1. Within the scope and for the performance of the services defined in the TOU, the Data Processor will process certain Personal Data on behalf of the Data Controller.<br>2. In addition to what may be provided in the TOU, the following shall apply to the Data Processor's processing of Personal Data on behalf of the Data Controller to fulfill the requirements under Applicable Data Protection Legislation. Data Subjects, data categories as well as the extent, nature, and purpose of data processing are determined by the TOU and "Data Controller's Processing Instructions" of this DPA. |
| **II. Processing of Personal Data** | Back to top |
| *The Data Processor will comply with all relevant requirements under Applicable Data Protection Legislation while following the Data Controller's instructions, including assisting the Data Controller in meeting legal obligations, refraining from actions that could breach Applicable Data Protection Legislation, and promptly notifying the Data Controller of any relevant communications or requests received from competent authorities.* | 1. The Data Processor and any person acting under its authority (e.g. personnel, Sub-processors, and persons acting under the Sub-processor's authority) undertake to only process Personal Data as instructed in writing by the Data Controller (see the "Data Controller's Processing Instructions" above). The Data Processor shall only process Personal Data to the extent necessary to fulfill its obligations under this DPA or Applicable Data Protection Legislation.<br>2. If the services are altered during the term of the TOU and such altered services involve new or amended processing of Personal Data, or if the Data Controller's instructions are otherwise changed or updated, the Data Controller shall instruct the Data |

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

Processor to update the "Data Controller's Processing Instructions" as appropriate before or at the latest in connection with the commencement of such processing or change.

3. The Data Processor shall comply with any Applicable Data Protection Legislation. The Data Processor shall keep itself updated on and comply with any changes in the Applicable Data Protection Legislation. The Data Processor shall make any necessary changes and amendments to this DPA required under Applicable Data Protection Legislation.
4. The Data Processor shall assist the Data Controller in fulfilling its legal obligations under Applicable Data Protection Legislation, including but not limited to:
   - protection of the rights of Data Subjects;
   - security of processing (Art. 32 GDPR);
   - notification of a personal data breach (Art. 33, 34 GDPR);
   - data protection impact assessment and the prior consultation (Art. 35, 36 GDPR); and
   - timely response to requests for exercising the Data Subject's rights to information regarding the processing of its Personal Data.

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

## III. Sub-processors

Back to top

*The Data Controller authorizes the Data Processor to engage Sub-processors to operate under the Data Controller's instructions. If the Data Processor intends to make changes to the current list outlined in the "Data Controller's Processing Instructions", it*

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 the "Data Controller's Processing Instructions" for the purposes specified therein. The Data Processor shall notify the Data Controller in

*will notify the Data Controller in advance and the Data Controller can object within 8 weeks.*

writing in advance of any changes, in particular before engaging other Sub-processors in which event the Data Processor shall without undue delay and no less than 8 weeks before transferring any Personal Data to a Sub-processor, inform the Data Controller in writing of the identity of such Sub-processor as well as the purpose for which it will be engaged.

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

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

## IV. Transfer to Third Countries

Back to top

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

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

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

## V. Security of Processing

Back to top

*The Data Processor ensures the security of Personal Data through specified technical and organizational measures (see Appendix 1). Further, the Data Processor will notify the Data Controller of any security incidents, restrict access to authorized personnel bound by confidentiality obligations, and appoint a designated contact person for data protection matters without undue delay.*

1. The Data Processor guarantees to implement and uphold appropriate technical and organizational measures according to the current state of the art to ensure an appropriate level of security for Personal Data and shall continuously review and improve the effectiveness of its security measures (See Appendix 1 hereunder). The Data Processor shall protect the Personal Data against destruction, modification, unlawful dissemination, or unlawful loss, alteration, or access. The Personal Data shall also be protected against all other forms of unlawful processing. With regard to the state of the art and the costs of implementation and taking into account the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, the technical and organizational measures to be implemented by the Data Processor shall include, as

appropriate:

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

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

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

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

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

6. The Data Processor shall ensure that access to Personal Data under this DPA is restricted to those of its personnel who directly require access to the Personal Data to fulfill the Data Processor's obligations under this DPA, the TOU or any existing agreement with the Data Controller. The Data Processor shall ensure that such personnel (whether employees or others engaged by the Data Processor):
   a. has the necessary knowledge of and training in the Applicable Data Protection Legislation to perform the contracted services; and
   b. is bound by a confidentiality obligation concerning the Personal Data to the same

extent as the Data Processor under this DPA.

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

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

## VI. Audit Rights

Back to top

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

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

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

## VII. Indemnification

Back to top

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

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

## VIII. Term

Back to top

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

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

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

## IX. Notices

Back to top

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

## X. Measures Upon Completion of Processing of Personal Data

Back to top

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

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

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

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

## XI. Definitions

Back to top

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

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

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

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

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

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

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

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

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

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

**"Processing"** means any operation or set of operations which is performed on Personal Data

or on sets of Personal Data, whether or not by automated means.

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

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

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

## XII. Final Provisions

Back to top

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

1. If the Data Controller and the Data Processor have entered into additional agreements in conflict with this DPA, the provisions of this DPA regarding the processing of Personal Data shall take priority. All other conflicting provisions shall be governed by the provisions of the TOU.

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

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

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

Back to top

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

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

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

## Document Information

*Document Owner:* VP Legal & Compliance

Version: V4.2

Date of Version: 2026-01-23