



Enterprise Data, **Unlocked.**

DATA PROCESSING AGREEMENT

Valority Technologies Ltd.

This Data Processing Agreement ("DPA") is hereby entered by and between Valority Technologies Ltd. and its Affiliates ("Valority" or "Company") and the Customer identified in the agreement executed between the parties ("Customer" or "you"), for the purpose of using the Services, as defined under the agreement between the parties ("Terms").

This DPA forms an integral part of the Terms. Capitalized terms not defined herein shall have the respective meanings given to them in the Terms.

This DPA sets forth the parties' responsibilities and obligations regarding the Processing of Personal Data during the course of the engagement between the parties.

1. Definitions

1.1. "Affiliates" means any entity which is controlled by, controls or is in common control with one of the parties.

1.2. "CCPA" means the California Consumer Privacy Act (Cal. Civ. Code 1798.100 - 1798.199) of 2018, as amended by the California Privacy Rights Act ("CPRA"), as well as all regulations promulgated thereunder from time to time.

1.3. The terms "Controller", "Processor", "Data Subject", "Processing" (and "Process"), and "Personal Data Breach" shall all have the same meanings as ascribed to them in EU Data Protection Law. The terms "Business", "Business Purpose", "Consumer", "Service Provider", "Sell" and "Share" shall have the same meaning as ascribed to them in the CCPA. "Data Subject" shall also mean and refer to "Consumer", as such terms are defined in the CCPA.

1.4. "Data Protection Law" means any and all applicable privacy and data protection laws and regulations (including, where applicable, EU Data Protection Law, UK Data Protection Law, and the CCPA) as may be amended or superseded from time to time.

1.5. "EU Data Protection Law" means (i) the EU General Data Protection Regulation (Regulation 2016/679) ("GDPR"); (ii) the EU e-Privacy Directive (Directive 2002/58/EC), as amended; (iii) any national data protection laws made under, pursuant to, replacing or succeeding (i) and (ii); (iv) any legislation replacing or updating any of the foregoing; and (v) any binding judicial or administrative interpretation, guidance, guidelines, codes of practice, or certification mechanisms issued by any relevant Supervisory Authority. "UK Data Protection Law" means the UK GDPR and the Data Protection Act 2018.

1.6. "Personal Data" or "Personal Information" means any information that can be related to, describes, is capable of being associated with, or can be used to directly or indirectly identify an individual or Data Subject, and that is Processed by Valority on behalf of Customer pursuant to the Terms, including by way of access to such data. Given the nature of the Services, Personal Data Processed on behalf of Customer consists primarily of aggregated and metric marketing and performance data, and may include limited identifiers such as Customer personnel contact details and online or customer identifiers contained in the data and systems Customer connects to the Services. The Services do not Process audio or video recordings or Special Categories of Personal Data.

1.7. "Security Incident" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. Any Personal Data Breach will comprise



Enterprise Data, **Unlocked.**

a Security Incident.

2. Parties' Roles

2.1. The parties agree and acknowledge that, with respect to the Processing of Personal Data under the Terms, Company acts as a Data Processor and Customer acts as a Data Controller. For the purpose of the CCPA (to the extent applicable), Customer is the Business and Valority is the Service Provider. Each party shall be individually responsible for complying with the obligations that apply to it under applicable Data Protection Law. In addition to its capacity as a Processor, Company is also a Controller of certain Personal Data related to the Customer, such as Customer's personnel contact details, which shall be used in accordance with Company's privacy policy available at: <https://valority.ai/legal/PrivacyPolicy> ("Privacy Policy").

2.2. The subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data, and the categories of Data Subjects are described in Schedule 1.

3. Representations and Warranties

The Customer represents and warrants that: (a) its Processing instructions shall comply with applicable Data Protection Law, and the Customer acknowledges that, taking into account the nature of the Processing, Valority is not in a position to determine whether the Customer's instructions infringe applicable Data Protection Law; and (b) it will comply with EU Data Protection Law, UK Data Protection Law, and the CCPA, specifically with regard to the lawful basis for Processing Personal Data. Valority represents and warrants that it shall Process Personal Data, as set forth under Article 28(3) of the GDPR, on behalf of the Customer solely for the purpose of providing the Services and for the pursuit of a Business Purpose under the CCPA, all in accordance with Customer's written instructions including the Terms and this DPA. Where Valority is required under applicable law to Process Personal Data other than as instructed by Customer, Valority shall use best efforts to inform the Customer of such requirement prior to Processing, unless prohibited under applicable law.

4. Processing of Personal Data and Compliance with Data Protection Law

4.1. The Customer represents and warrants that Special Categories of data shall not be Processed or shared in connection with the Services, unless agreed in writing by Valority. Unless otherwise agreed in writing, the Customer shall not share with Valority any Personal Data relating to children under 16 years old.

4.2. The Customer accepts that Data Subjects do not have a direct relationship with Valority and that Valority relies on Customer's lawful basis. Where consent is required under Data Protection Law, the Customer shall obtain valid consent from Data Subjects and present all necessary notices to enable lawful transfer and Processing of Personal Data by Customer and Valority, and, where applicable, provide Data Subjects with the ability to opt out. The Customer shall maintain records of consents and withdrawals and make them available to Valority promptly upon request.

4.3. Automated decision-making. The Services provide decision-support and recommendations only. Valority does not, on Customer's behalf, carry out any Processing that produces legal effects concerning Data Subjects, or that similarly significantly affects them, based solely on automated processing. Customer is responsible for ensuring meaningful human involvement before acting on any Output.

5. Confidentiality

Valority shall ensure that personnel authorized to Process the Personal Data are subject to binding obligations of confidentiality, have received appropriate data protection training, and may access Personal Data only on a need-to-know basis to provide the Services.

6. Sub-processors

6.1. Customer provides Valority with a general authorization to engage sub-processors to Process Personal Data in connection with the Services, including cloud infrastructure providers, AI model providers, and operational service providers. A current list of sub-processors is available on request or via the Documentation.

6.2. Valority shall impose on each sub-processor, by written contract, data protection obligations no less protective than those set out in this DPA, in particular the obligations under Article 28(3) GDPR, and shall remain fully liable to Customer for the acts and omissions of its sub-processors.

6.3. Valority shall provide a mechanism to notify Customer of any intended addition or replacement of a sub-processor, giving Customer a reasonable period to object on legitimate data protection grounds. If the parties cannot resolve a reasonable objection, Customer may, as its sole remedy, terminate the affected part of the Services.

7. Rights of Data Subject and Parties' Cooperation Obligations

Where Valority receives a request from a Data Subject or an applicable authority in respect of Personal Data Processed by Valority, Valority will, where relevant, direct the Data Subject or authority to the Customer to enable the Customer to respond directly, unless otherwise required under applicable law. The parties shall provide each other with commercially reasonable cooperation and assistance in handling such requests, to the extent permitted under Data Protection Law, including assistance with data protection impact assessments and prior consultations where required by Articles 32-36 GDPR.

8. No Sale of Personal Information

Any sharing of Personal Data between the parties is made solely for fulfilling a Business Purpose, and Valority does not receive or Process any Personal Data as consideration for the Services. Such Processing shall not be considered a "Sale" or "Share" of Personal Information under the CCPA. Valority will not retain, use, or disclose Personal Data for any purpose other than performing the Services. It is the Customer's sole responsibility to determine whether its sharing or transferring of Personal Data constitutes a Sale or Share under the CCPA and to comply with the applicable requirements, including honoring opt-out signals where applicable.

9. Technical and Organizational Measures

Valority confirms that it has implemented and will maintain appropriate physical, technical and organizational measures to protect the Personal Data as required under Data Protection Law (including Article 32 GDPR), to ensure lawful Processing and to safeguard Personal Data from unauthorized, unlawful or accidental Processing, access, disclosure, loss, alteration or destruction, consistent with Valority's Security Policy.



Enterprise Data, **Unlocked.**

10. Security Incident

Valority will notify the Customer without undue delay upon becoming aware of any confirmed Security Incident involving Personal Data in Valority's possession or control. Such notification or response shall not be construed as an acknowledgment of fault or liability. Valority will, in connection with any such Security Incident: (i) take steps necessary to contain, remediate, minimize the effects of, and investigate the Security Incident and identify its cause; (ii) cooperate with the Customer and provide reasonable assistance and information; and (iii) notify the Customer in writing of any request, inspection, audit or investigation by a supervisory or other authority.

11. Audit Rights

Valority shall make available, solely upon prior written notice and no more than once per year, to a reputable auditor nominated by the Customer, information necessary to reasonably demonstrate compliance with this DPA, and shall allow for audits, including inspections, solely in relation to the Processing of the Personal Data ("Audit"). The auditor shall be subject to this DPA and standard confidentiality obligations. Valority may object to an auditor it reasonably believes is not suitably qualified or independent, is a competitor of Valority, or is otherwise unsuitable ("Objection Notice"), in which case the Customer will appoint a different auditor or conduct the Audit itself. Customer shall bear all expenses of the Audit and shall ensure that it and its auditors avoid causing damage or disruption to Valority's premises, equipment, personnel and business. All conclusions of an Audit shall be confidential and reported back to Valority promptly.

12. International Data Transfers

12.1. Valority is established in Israel, which benefits from a European Commission adequacy decision for transfers of Personal Data from the EEA.

12.2. Where Personal Data is transferred to a country that is not subject to an adequacy decision, the parties shall ensure an appropriate transfer mechanism applies. Such mechanisms may include the European Commission's Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914) ("SCCs"), the UK International Data Transfer Addendum to the SCCs, and the Swiss addendum, together with any supplementary measures required under applicable Data Protection Law. Such mechanisms are deemed incorporated into this DPA where required and shall apply to the relevant transfer; in the event of conflict, the applicable transfer mechanism shall prevail to the extent necessary for compliance.

13. Return and Deletion of Personal Data

On termination or expiry of the Terms, and at Customer's choice, Valority shall delete or return all Personal Data Processed on Customer's behalf and delete existing copies, unless retention is required by applicable law. In any event, Personal Data shall not be retained longer than necessary to provide the Services and no longer than twelve (12) months following termination, except where retention is required by law. This Section gives effect to Article 28(3)(g) GDPR.

14. Conflict

In the event of a conflict between the terms of this DPA and the Terms, this DPA shall prevail solely with respect to the Processing of Personal Data and to the extent of the conflict.

SCHEDULE 1

DETAILS OF PROCESSING OF CONTROLLER PERSONAL DATA

This Schedule 1 includes the details of Processing required by Article 28(3) GDPR.

Subject matter and duration of the Processing:

Processing is carried out in connection with the provision of the Services. The duration shall be the duration of the Term, subject to Section 13 (Return and Deletion of Personal Data).

Nature and purpose of the Processing:

To provide the Services to the Customer: ingesting, analyzing, and generating insights, forecasts, and recommendations from the data and systems the Customer connects, for the purpose of marketing and growth decision-support.

Types of Personal Data Processed:

Primarily aggregated and metric marketing and performance data. To the extent Personal Data is present, it is limited to: (i) contact information and account data of Customer's personnel and Authorized Users (e.g., name, work email, username, access authorizations); and (ii) online or customer identifiers and related engagement, campaign, or transaction records contained in the systems the Customer connects to the Services. No Special Categories of Personal Data and no audio or video recordings are Processed.

Categories of Data Subjects:

Customer's personnel and Authorized Users; and, to the extent present in connected data, Customer's own customers, prospects, and website or application users.

Location of Processing:

Customer Data is hosted and processed in cloud regions located in the European Union (EU/EEA) and the United States. Valority personnel located in Israel may access Personal Data where necessary to provide and support the Services; Israel benefits from a European Commission adequacy decision. Regional data residency (for example, EU-only hosting) may be available where agreed in an Order Form.

Retention:

Personal Data is retained for the duration of the Term and deleted or returned thereafter in accordance with Section 13, and in any event no longer than twelve (12) months following termination, unless retention is required by law.