**Datawarehouse.io**

**Data Processing Agreement**

**Effective Date: February 2, 2023**

This Data Processing Agreement and its annexes (“**DPA**”) reflects the agreement between Datawarehouse.io LLC ("**Datawarehouse.io**", "**we**", "**us**", or "**our**") and registered Subscribers ("**Subscribers**", "**you**" or "**your**") with respect to the processing of Personal Data by Datawarehouse.io on your behalf in connection with your access and ongoing use of Datawarehouse.io Integrations.

This DPA is made pursuant to the Datawarehouse.io Terms and Conditions ([https://datawarehouse.io/terms-conditions](https://datawarehouse.io/TERMS-CONDITIONS)) (“**Agreement**”) and supplements and forms an integral part of the Agreement and is effective as of your first use of any Datawarehouse.io Integration. All terms and conditions of the Agreement shall apply to this DPA unless clearly stated otherwise herein. Should a conflict between this DPA and the Agreement exist, the terms of this DPA shall control.

**Acceptance of this DPA**

Your access to and use of the Integrations is conditional on your acceptance of the terms and conditions of this DPA. By accessing and using the Integrations, you agree on your own behalf, and on behalf of any Authorized Affiliates on whose behalf you may act, to accept and abide by this DPA. If you do not agree with all terms and conditions of this DPA, please do not access or use any Datawarehouse.io Integrations.

**Modification to this DPA**

We reserve the right to modify this DPA at any time by posting an updated DPA on the Site. We may also, at our sole discretion, provide active Subscribers with an email notice of changes. You are responsible for regularly reviewing this DPA and your continued use of the Integrations after the effective date of any change shall constitute your acceptance of the updated DPA. If any modification is unacceptable to you, you shall cease using the Integration. If you have any questions about this DPA, or if you need a signed copy of this DPA, including the full text of any referenced SCCs or Annexes, you may contact us at help@datawarehouse.io**.**

1. **Definitions**. Capitalized terms not defined herein have the meaning set forth in the Agreement.

“**Authorized Affiliates**” means any of your Affiliates that you have provided access to the Integrations but who are not Subscribers as defined in the Agreement.

“**California Consumer Privacy Protection Act**” or “**CCPA**” means California Civil Code § 1798.100 et seq.

“**California Personal Information**” or “**CA Personal Information**” means Personal Data that is subject to the protection of the CCPA.

"**Consumer**," "**Business**," "**Sell**," and "**Service** **Provider**" will have the meanings given to them in the CCPA.

“**Controller**” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

“**Customer Personal Data**” means the Personal Data about you, your personnel, and/or your customers that we Process for or on behalf of you in order to provide the Integrations under the Agreement.

“**Data Protection Laws**” means data protection laws or privacy laws of any country or state applicable to Datawarehouse.io’s and/or Subscriber’s Processing of Customer Data, including Personal Data.

“**Data Subjects**” means the identified or identifiable natural person to whom Personal Data relates.

“**European Data**” means Personal Data that is subject to the protection of European Data Protection Laws.

“**European Data Protection Laws**” means data protection laws applicable in Europe, including: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("GDPR"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector;(iii) applicable national implementations of (i) and (ii), or in respect of the United Kingdom, any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the United Kingdom leaving the European Union; and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance, in each case, as may be amended, superseded or replaced.

“**European Union**” or “**EU**” means the European Union, the European Economic Area and/or their member states, Switzerland, and the United Kingdom.

“**Personal Data**” means any information relating to an identified or identifiable natural person (‘Data Subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“**Personal Data Breach**” means a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed through Integrations or the systems that compromises the security, confidentiality or integrity of such Personal Data.

“**Process**” or “**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, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure or destruction.

“**Processor**” means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

“**Sensitive Data**” means (i) any patient, medical or other protected health information regulated by HIPAA or any similar federal or state laws, rules or regulations; or (ii) any other information subject to regulation or protection under specific laws such as the Gramm-Leach-Bliley Act (or related rules or regulations).

“**Special Category Data**” means any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

“**Standard Contractual Clauses**” or “**SCCs**” means the standard contractual clauses annexed to the European Commission’s Decision (EU) 2021/914 of 4 June 2021 currently found at [https://commission.europa.eu/publications/ standard-contractual-clauses-international-transfers\_en](https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en), and as may be amended.

“**Subcontractor**” means Datawarehouse.io’s service providers, agents, subcontractors, and all other persons, entities, or organizations, exclusive of you employees or Third-Party Service providers who are subject to your direction, supervision, and control.

“**Swiss DPA**” means the Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance, as may be amended.

“**UK GDPR**” means the International Data Transfer Addendum issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act of 2018 currently found at [https://ico.org.uk/media/for-organisations/documents/ 4019539/international-data-transfer-addendum.pdf](https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf), as may be amended.

“**Sub-Processor**” means any Subcontractors engaged by Datawarehouse.io to Process Customer Data who are identified by Datawarehouse.io in the Agreement or otherwise approved or acknowledged in writing by you.

1. **Scope**. This DPA applies if and to the extent Customer Data contains Personal Data and is received by Datawarehouse.io from or on behalf of you as a data Processor while providing the Integrations. Datawarehouse.io is not responsible or liable for compliance or non-compliance with any laws applicable to your industry that are not generally applicable to us.
2. **Term**. This DPA begins on the date we first receive or have access to Customer Data and continues thereafter for the period during which we are a data Processor and have possession or access to Customer Data in connection with the Integrations until expiration or cancellation of the Integrations.
3. **Datawarehouse.io Responsibilities**
	1. **Purpose**. Datawarehouse.io will Process Customer Data, including Personal Data, solely for the purpose of providing the Integrations in accordance with the Agreement and this DPA, or as otherwise instructed by you.
	2. **Compliance**. Datawarehouse.io will comply with all applicable Data Protection Laws and any reasonable instructions provided by you in the Processing of Customer Data. If Datawarehouse.io cannot provide such compliance for whatever reason, it agrees to promptly inform you of its inability to comply. If for any reason Datawarehouse.io, in its sole discretion, believes that any one or more of the available Integrations cannot comply with applicable Data Protection Laws, then Datawarehouse.io reserves the right to cease all Processing of your Customer Data or stop providing such Integrations to you or to customers generally until we are either able to comply or you provide us with instructions that do violate applicable law. We shall not be liable for the failure to provide the Integrations should we choose to invoke our rights provided in this section, and your sole remedy shall be the right to cancel any applicable Subscription Services.
	3. **Safeguards**. Datawarehouse.io will implement and maintain policies, procedures, and practices that satisfy the applicable requirements set forth in this DPA.
4. **Subscriber Responsibilities**
	1. **Subscriber Compliance**. You are responsible for compliance with your requirements under the applicable Data Protection Laws with respect to Customer Data and the instructions you provide us related to such Customer Data. Without limiting the generality of the foregoing, you are solely responsible for: (i) the accuracy, quality, integrity, and legality of your Customer Data and the means by which you acquire Customer Data; (ii) ensuring you have the right to transfer, or provide access to, Customer Data in order for us to provide the Integrations; and (iii) ensuring that any instructions that you provide to us regarding the Processing of Customer Data comply with all applicable laws. You will inform us without undue delay if you are not able to comply with your responsibilities under this section or applicable Data Protection Laws.
	2. **Specific Disclaimers**. You recognize and agree that hosting content online involves risks of unauthorized disclosure or exposure and that, in using the Integrations, you assume such risks. We shall not, in any way, be responsible for any intentional or unintentional misuse of Customer Data by you (including your employees, subsidiaries, or Affiliates) and/or by your authorized users or Third-Party Service providers to whom you have granted access to Customer Data. You are solely responsible for granting access to the Integrations by providing Credentials to your users.
	3. **Customer Instructions**. You acknowledge and agree that the instructions contained in the Agreement, any Product Specific Terms, and this DPA related to the Processing of Customer Data (“**Instructions**”) constitute the complete instructions from you regarding our Processing of Customer Data. To the extent any additional instructions from you are consistent with the Instructions, we will Process Customer Data in accordance with the additional instructions. To the extent any additional instructions from you are inconsistent with the Instructions, we may, at our discretion, refuse to honor such additional instructions to the maximum extent permitted under applicable Data Protection Laws.
	4. **No Reliance**.We cannot ensure or in any way guarantee that the Integrations and the security of the systems that provide the Integrations will meet your specific data security requirement, whether to your customers or under applicable Data Protection Laws. You are responsible for independently evaluating whether the Integrations adequately meet your obligations.
	5. **No Special Category Data**. The Integrations may not be adequate to protect Sensitive Data or Special Category Data that imposes specific data security or data protection obligations. You acknowledge and agree that transmitting, processing, or otherwise making such data available to the Integrations is entirely at your own risk. DATAWAREHOUSE.IO SHALL HAVE NO OBLIGATION TO YOU WITH REGARDS TO PROCESSING OF SENSITIVE DATA OR SPECIAL CATEGORY DATA BEYOND THE OBLIGATIONS SET FORTH IN THE AGREEMENT AND/OR THIS DPA.
5. **Processing**. Datawarehouse.io may Process Customer Data as necessary to provide the Integrations, including where applicable for hosting and storage; backup and recovery; issue resolution; applying new product or system versions, patches, updates, and upgrades; monitoring, and testing system use and performance; IT security purposes including incident management; maintenance and performance of technical support systems; and migration, implementation, configuration, and performance testing. Datawarehouse.io shall not: (i) modify Customer Data other than as necessary to provide the Integrations; (ii) disclose Customer Data except as compelled by law or as expressly permitted by Subscriber; or (iii) access Customer Data except to provide the Integrations, address service or technical problems, or at Subscriber’s request in connection with customer support matters.
6. **Sub-Processors**. Datawarehouse.io may subcontract its Processing work that relates to Personal Data under the Agreement to Third-Party Service Providers identified in the Agreement or as listed on our Site ([https://www.datawarehouse.io /subprocessors/](https://www.datawarehouse.io)). Subject to applicable Data Protection Laws, Subscriber agrees that Datawarehouse.io may later use Sub-Processors not identified in the Agreement or listed on our Site. We will require that all our Sub-Processors maintain adequate measures reasonably appropriate to such Sub-Processor’s storage, maintenance or processing activities that comply in all material respects with the relevantobligations in this DPA (including, where appropriate, the Standard Contractual Clauses), to the extent applicable to the nature of the services provided by such Sub-Processors. We will remain responsible for each Sub-Processor’s compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause us to breach any of its obligations under this DPA.
7. **International Transfers**. Unless otherwise provided in the Agreement, our [Regional Data Hosting Policy](https://www.datawarehouse.io/regional-data-hosting), or our Product Specific Terms, Datawarehouse.io may Process Customer Data globally as necessary to provide the Integrations. If you purchase an Integration that is identified on the Site as being hosted in the United States, and if you are located anywhere other than the United States, your access and use of such Integration constitutes your consent to our transferring, and the subsequent storage of, your Customer Data from your country of origin to the United States. If the Agreement or Product Specific Terms indicate a specific geographic location where your Customer Data will be stored and hosted (“**Country of Origin**”), then any transfer of Customer Data, including Personal Data, outside of the Country of Origin by us (if any) will only be done through your written permission and in compliance with the relevant provisions of the Data Protection Laws in the originating country.
8. **Cooperation and Inquiries**. One Party will promptly inform the other Party if it receives any inquiry, complaint, or claim from any court, governmental official, third parties, or individuals arising out of the Subscription Services and will provide the other Party reasonable support and cooperation in a timely manner in responding to any request. Should Datawarehouse.io directly receive a request or inquiry from a Data Subject that has identified you as the Controller, Datawarehouse.io will promptly pass on such requests to you without responding to the Data Subject. Should you, on the basis of applicable law, be obliged to provide access or information to a Data Subject about the Processing of Personal Data relating to him or her, Datawarehouse.io will reasonably assist you in providing such access or information.
9. **Confidentiality and Information Security**. We have implemented and will maintain appropriate technical and organizational security measures for the Processing of Personal Data designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. These security measures govern all areas of security applicable to the Integrations, including physical access, system access, data access, transmission and encryption, input, data backup, data segregation and security oversight, enforcement, and other security controls and measures. All Datawarehouse.io employees, as well as any Sub-Processors that Process Personal Data, are subject to appropriate written confidentiality arrangements or are otherwise bound by statutory obligations of confidentiality.
10. **Data Breach Incidents**. If we become aware of a Personal Data Breach while providing the Integrations under the Agreement, we will inform you without undue delay. We will take appropriate measures to address the Personal Data Breach, including, where appropriate, securing Personal Data, and will work in good faith to reduce risk to the Data Subjects whose Personal Data was involved. Applicable Data Protection Laws may impose a duty to inform the competent authorities or affected Data Subjects in the event of the loss or unlawful disclosure of Personal Data or access to it, and we agree to provide you with sufficient information to allow you to meet any obligations to report or inform Data Subjects of the Personal Data Breach under applicable Data Protection Laws. We will cooperate with you and take reasonable steps as necessary to assist in the investigation, mitigation, and remediation of each Personal Data Breach. You agree that you are responsible for and will coordinate the messaging related to any privacy violation, security breach, or data breach incident with us prior to making any public disclosures.
11. **Deletion of Customer Data**. Datawarehouse.io will, except to the extent provided in the Agreement or prohibited by applicable law, destroy and delete all Customer Data subject to Processing in accordance with the timeframes set forth in our [Product Specific Terms](http://www.datawarehouse.io/product-specific-terms), and the right to have Customer Data returned to you shall expire after such date or time frame.
12. **Legal Requirements**. We may be required by law to provide access to Personal Data, such as to comply with a subpoena or other legal process, or to respond to government requests, including public and government authorities for national security and/or law enforcement purposes. We agree to promptly inform you of requests for access to Customer Data, unless otherwise required by law.
13. **Additional Provisions for EU Subscribers**
	1. **Role of the Parties**. You acknowledge that for the purposes of EU Data Protection Laws and this DPA, you are the Controller and we are the Processor with respect to Customer Data.
	2. **Objections to New Sub-Processors**. We will give you the opportunity to object to the engagement of new Sub-Processors on reasonable grounds relating to the protection of Customer Data within thirty (30) days of notifying you in accordance with the ‘Sub-Processors’ section. If you do notify us of such an objection, the parties will discuss your concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, we will, at our sole discretion, either not appoint the new Sub-Processor, or permit you to suspend or terminate the affected Integration in accordance with the termination provisions of the Agreement without liability to either party (but without prejudice to any fees incurred by you prior to suspension or termination). The parties agree that by complying with this subsection, Datawarehouse.io fulfills its obligations under Section 9 of the Standard Contractual Clauses.
	3. **Sub-Processor Agreements**. For the purposes of Clause 9(c) of the Standard Contractual Clauses, you acknowledge that we may be restricted from disclosing Sub-Processor agreements but we will use reasonable efforts to require any Sub-Processor we appoint to permit it to disclose the Sub-Processor agreement to you and will provide (on a confidential basis) all information we reasonably can.
	4. **Data Protection Impact Assessments and Consultation with Supervisory Authorities**. To the extent that the required information is reasonably available to us, and you do not otherwise have access to the required information, we will provide reasonable assistance to you with any data protection impact assessments, and prior consultations with supervisory authorities (for example, the French Data Protection Agency (CNIL), the Berlin Data Protection Authority (BlnBDI), the UK Information Commissioner's Office (ICO)), or other competent data privacy authorities to the extent required by EU Data Protection Laws.
	5. **Data Transfers**. Other than for limited exclusions, as provided in our [Regional Data Hosting Policy](https://www.datawarehouse.io/regional-data-hosting), we will not transfer European Data to any country or recipient not recognized as providing an adequate level of protection for Personal Data (within the meaning of applicable EU Data Protection Laws), unless we first take all such measures as are necessary to ensure the transfer is in compliance with applicable EU Data Protection Laws. Such measures may include (without limitation) transferring such data to a recipient that: (i) is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data; (ii) has achieved binding corporate rules authorization in accordance with EU Data Protection Laws; (iii) has executed appropriate Standard Contractual Clauses in each case as adopted or approved in accordance with applicable EU Data Protection Laws. You acknowledge that in connection with the provision of the Integrations, Datawarehouse.io may be a recipient of European Data in the United States. The parties agree that the Standard Contractual Clauses will be incorporated by reference and form part of the Agreement as follows:
		1. **EEA Transfers**. In relation to European Data that is subject to the GDPR, (i) you are the "data exporter" and we are the "data importer"; (ii) the Module Two terms apply to the extent you are a Controller of European Data and the Module Three terms apply to the extent you are a Processor of European Data; (iii) in Clause 7, the optional docking clause applies; (iv) in Clause 9, Option 2 applies and changes to Sub-Processors will be notified in accordance with the ‘Sub-Processors’ section of this DPA; (v) in Clause 11, the optional language is deleted; (vi) in Clauses 17 and 18, the parties agree that the governing law and forum for disputes for the Standard Contractual Clauses will be determined in accordance with the ‘Governing Law’ section of the Agreement; (vii) the Annexes of the Standard Contractual Clauses will be deemed completed with the information set out in the Annexes of this DPA; and (viii) if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA the Standard Contractual Clauses will prevail to the extent of such conflict.
		2. **UK Transfers**. In relation to European Data that is subject to the UK GDPR, the Standard Contractual Clauses will apply and the following modifications: (i) the Standard Contractual Clauses will be modified and interpreted in accordance with the UK Addendum, which will be incorporated by reference and form an integral part of the Agreement; (ii) Tables 1, 2 and 3 of the UK Addendum will be deemed completed with the information set out in the Annexes of this DPA and Table 4 will be deemed completed by selecting “neither party”; and (iii) any conflict between the terms of the Standard Contractual Clauses and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.
		3. **Swiss Transfers**. In relation to European Data that is subject to the Swiss DPA, the Standard Contractual Clauses will apply and the following modifications: (i) references to "Regulation (EU) 2016/679" will be interpreted as references to the Swiss DPA; (ii) references to "EU", "Union" and "Member State law" will be interpreted as references to Swiss law; and (iii) references to the "competent supervisory authority" and "competent courts" will be replaced with the "the Swiss Federal Data Protection and Information Commissioner " and the "relevant courts in Switzerland."
		4. **Other Transfer Mechanisms**. In the event that we adopt an alternative transfer mechanism (including any new or successor version of the EU-US Privacy Shield) for transfers of European Data, such alternative transfer mechanism will apply automatically instead of the Standard Contractual Clauses described in this DPA (but only to the extent such alternative transfer mechanism complies with EU Data Protection Laws), and you agree to execute such other documents or take such action as may be reasonably necessary to give legal effect such alternative transfer mechanism.
		5. **Non-Compliance**. If we cannot comply with our obligations under the Standard Contractual Clauses or would be in breach of any warranties under the Standard Contractual Clauses or UK Addendum (as applicable) for any reason, and you intend to suspend the transfer of European Data to us or terminate the Standard Contractual Clauses, or UK Addendum, you agree to provide us with reasonable notice to enable us to cure such non-compliance and reasonably cooperate with us to identify what additional safeguards, if any, may be implemented to remedy such non-compliance. If we have not or cannot cure the non-compliance, you may suspend or terminate the affected part of the Integration in accordance with the Agreement without liability to either party (but without prejudice to any fees you have incurred prior to such suspension or termination).
	6. **Inspection and Audit Rights**
		1. **Demonstration of Compliance**. We will make all information reasonably necessary to demonstrate compliance with this DPA available to you and allow for and contribute to audits, including inspections conducted by your auditor in order to assess compliance with this DPA. You acknowledge and agree that you will exercise your audit rights under this DPA and Clause 8.9 of the Standard Contractual Clauses by instructing us to comply with the audit measures described in this 'Demonstration of Compliance' section. You acknowledge that the Integrations are hosted by one or more of our Sub-Processors who maintain independently validated security programs. At your written request, we will provide written responses (on a confidential basis) to all reasonable requests for information made by you necessary to confirm our compliance with this DPA, provided that you will not exercise this right more than once per twelve (12) month period unless you have reasonable grounds to suspect non-compliance with the DPA.
		2. **Form of Audit**. You may inspect, at your expense, our operating facilities or conduct an audit of our security, technical, and organizational procedures used for Processing Customer Data to verify compliance with this DPA (“**Audit**”). Unless otherwise required by applicable Data Protection Laws, you may Audit our compliance with this DPA once per twelve (12) month period, unless a violation of our obligations is found, in which case you may conduct another Audit within six (6) months. The Audit may be conducted by your data protection officer or a mutually accepted authorized representative or third party auditor, and any such third-party officer, representative, or auditor must sign a confidentiality agreement acceptable to us or otherwise be bound by a statutory or legal confidentiality obligation. We agree to provide you with any reasonably necessary information and documents during the Audit. All Audits will be performed during normal working hours and in such a way that the Audit does not disrupt or compromise our normal business operations. We will cooperate with any Audit ordered by a relevant regulator that arises from our performance under the Agreement.
		3. **Scope of Audit**. Prior to any Audit, we must mutually agree in writing on the scope of the Audit, which must describe the proposed scope, duration, and start date of the Audit. You must provide prior written notice, including a written explanation of the reason for the Audit, to us no later than thirty (30) days before any such Audit commences. Prior to any Audit, both parties shall agree to pursue, in good faith, other means of reconciling the documents that would render such Audits not necessary. Such third party Auditor may not disclose to you anything other than the results of our compliance or non-compliance with the Audit and any Audit shall not entitle you to view, or in any way access records and/or processes: (i) not directly related to your Customer Data Processed by us; (ii) not directly related to the Integrations provided to you under the Agreement; (iii) in violation of applicable laws; and/or (iv) in violation of our confidentiality obligations owed to a third party.
		4. **Disclosure of Audit**. You agree to provide us with the results of the Audit, including any documented reports, which shall be subject to the confidentiality terms of the Agreement. You may use the Audit reports only for the purpose of meeting your requirements in accordance with applicable Data Protection Laws or for confirming our compliance with this DPA.
		5. **Sub-Processor Audits**. You may request that we Audit any Sub-Processor or provide confirmation that such an Audit has occurred (or, where available, obtain or assist you in obtaining a third-party audit report concerning the Sub-Processor’s operations) to verify compliance with the Sub-Processor’s obligations. You will also be entitled, upon written request, to receive copies of the relevant privacy and security terms of our agreement with any Sub-Processors that may Process your Customer Data.
		6. **Data Protection Impact Assessment**. We will provide reasonable assistance to you with any data protection impact assessments which you reasonably consider to be required by article 35 or 36 of the GDPR or equivalent provisions of any Data Protection Law, in each case solely in relation to Processing of Customer Data by us.
14. **Additional Provisions for California Personal Information**. When Processing CA Personal Information in accordance with your Instructions, you agree that you are a Business and we are a Service Provider for the purposes of the CCPA, and that we will Process CA Personal Information as a Service Provider strictly for the purpose of providing the Integrations under the Agreement ("Business Purpose") or as otherwise permitted by the CCPA, including as described in our Privacy Policy. We shall not (a) Sell any CA Personal Information other than use Google Analytics; (b) retain, use, or disclose any CA Personal Information for any purpose other than for the specific purpose of providing the Integration, including retaining, using, or disclosing the CA Personal Information for a commercial purpose (as defined in the CCPA) other than provision of the Integrations; or (c) retain, use, or disclose the CA Personal Information outside of the direct business relationship between us and you.
15. **General Provisions**
	1. **Severability**. If any provision of this DPA is held invalid or unenforceable by any court of competent jurisdiction, the parties shall mutually agree on an alternate, legally valid and enforceable provision. The remainder of this DPA shall continue in full force and effect to the extent that continued operation without the invalid or unenforceable provision is consistent with the intent of the parties.
	2. **Disclaimer**. DATAWAREHOUSE.IO SHALL NOT BE LIABLE FOR: (I) VIOLATION OF ANY APPLICABLE DATA PROTECTION LAW, (II) PERSONAL DATA BREACH, OR (III) VIOLATION OF ANY PRIVACY OR INTELLECTUAL PROPERTY RIGHTS, ASSOCIATED WITH CUSTOMER DATA STORED ON YOUR SERVERS OR CAUSED BY YOUR ACTS, OMISSIONS, OR NEGLIGENCE.
	3. **Limitation of Liability**. Each party and each of their Affiliates' liability, taken in aggregate, arising out of or related to this DPA and the Standard Contractual Clauses (where applicable), whether in contract, tort, or under any other theory of liability, will be subject to the limitations and exclusions of liability set out in the 'Limitation of Liability' section of the Agreement and any reference in such section to the liability of a party means aggregate liability of that party and all of its Affiliates under the Agreement (including this DPA). In no event will either party's liability be limited with respect to any individual's data protection rights under this DPA (including the Standard Contractual Clauses) or otherwise. IN NO EVENT WILL DATAWAREHOUSE.IO’S LIABILITY TO YOU FOR A BREACH OF CUSTOMER DATA EXCEED ONE MILLION DOLLARS ($1,000,000).
	4. **Governing Law**. This DPA will be governed by the choice of law and jurisdiction provisions contained in the Agreement unless otherwise required by applicable Data Protection Laws.
	5. **Indemnity**. In addition to any indemnification provisions provided in the Agreement, the parties further agree that if one party is held liable for a violation of Data Protection Laws committed by the other party, the latter will, to the extent to which it is liable, indemnify the other party for any cost, charge, damages, expenses, or loss it has incurred as part of its obligations; and (ii) the limitations of liability provided in the Agreement, including the aggregate liability cap, applies to this Section to the maximum extent permitted by applicable law.
	6. **Integration**. Except as otherwise set forth in this DPA, all terms and conditions contained in the Agreement and not amended herein shall remain in full force and effect. In the event of a conflict between the Agreement and this DPA or any other confidentiality term in an agreement between us, the order of precedence in respect of the Processing of Customer Data shall be: this DPA and then the Agreement.

**Annex 1 - Details of Processing**

This Annex forms part of the DPA.

1. **List of Parties**
	1. **Data exporter:**

Name: The Subscriber, as defined in the Datawarehouse.io Terms and Conditions (on behalf of itself and Authorized Affiliates)

Address: The Subscriber’s address, as set out in the Subscriber’s User Account

Contact person’s name, position and contact details: The Subscriber’s contact details, as set out in the Subscriber’s User Account

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Subscriber’s use of the Datawarehouse.io Integrations under the Datawarehouse.io Terms and Conditions

Role (controller/processor): Controller

* 1. **Data importer:**

Name: Datawarehouse.io LLC

Address: 10810 Katy Freeway, Suite 101, Houston, TX 77043

Contact person’s name, position and contact details: James Elmer, Chief Technology Officer, Datawarehouse.io, 10810 Katy Freeway, Suite 101, Houston, TX 77043

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Subscriber’s use of the Datawarehouse.io Integrations under the Datawarehouse.io Terms and Conditions

Role (controller/processor): Processor

1. **Nature and Purpose of Processing**

We will Process Personal Data as necessary to provide the Integrations pursuant to the Agreement, as further specified in any Product Specific Terms, and as further instructed by you in your use of the Integrations.

1. **Duration of Processing**

Subject to the "Deletion of Customer Data" section of this DPA, we will Process Personal Data for the duration of your use of the Integration, unless otherwise agreed in writing.

1. **Categories of Data Subjects**

You may submit Personal Data in the course of using the Integrations, the extent of which is determined and controlled by you in your sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects: Your Contacts and other end users including your employees, contractors, collaborators, customers, prospects, suppliers, and subcontractors. Data Subjects may also include individuals attempting to communicate with or transfer Personal Data to your end users.

1. **Categories of Personal Data**

You may submit Personal Data to the Integrations, the extent of which is determined and controlled by you in your sole discretion, and which may include but is not limited to the following categories of Personal Data:

* 1. Contact Information (as defined in the Agreement).
	2. Any other Personal Data submitted by, sent to, or received by you, or your end users, via the Integrations.
1. **Sensitive Data or Special Categories of Data (if appropriate)**

The parties do not anticipate the transfer of Sensitive Data or Special Category Data.

1. **Processing Operations**

Personal Data will be Processed in accordance with the Agreement or this DPA, and may be subject to the following Processing activities:

* 1. Storage and other Processing necessary to provide, maintain, and improve the Integrations provided to you; and/or
	2. Disclosure in accordance with the Agreement, this DPA, and/or as compelled by applicable laws.
1. **Competent Supervisory Authority**

For the purposes of the Standard Contractual Clauses, the supervisory authority that will act as competent supervisory authority will be determined in accordance with the GDPR.

**Annex 2 - Security Measures**

This Annex forms part of the DPA.

Datawarehouse.io currently observes the Security Measures described in this Annex 2. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Agreement.

1. **Access Control**
	1. **Preventing Unauthorized Integration Access**

Outsourced processing: We host our Integrations with outsourced cloud infrastructure providers. Additionally, we maintain contractual relationships with service providers in order to provide the Integrations in accordance with our Data Processing Agreement. We rely on contractual agreements, privacy policies, and service provider compliance programs in order to protect Customer Data Processed or stored by these service providers.

Physical and environmental security: We host our Integration infrastructure with multi-tenant, outsourced infrastructure providers.

Authentication: We implement a uniform password policy for our Integrations. Subscribers who interact with the Integrations via the Platform must authenticate before accessing non-public Customer Data.

Authorization: Customer Data is stored in multi-tenant storage systems accessible to Subscribers via only application user interfaces and application programming interfaces. You are not allowed direct access to the underlying application infrastructure. The authorization model in each of our Integrations is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user’s permissions against the attributes associated with each data set.

* 1. **Preventing Unauthorized Product Use**

We implement industry standard access controls and detection capabilities for the internal networks that support our Integrations.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the Integration infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Intrusion detection and prevention: We implement a Web Application Firewall (WAF) solution to protect hosted Customer Data and internet-accessible Integrations. The WAF is designed to identify and prevent attacks against publicly available network services.

Static code analysis: Security reviews of code stored in our source code repositories are performed, checking for coding best practices and identifiable software flaws.

* 1. **Limitations of Privilege & Authorization Requirements**

Integration access: A subset of Datawarehouse.io employees have access to the Integrations and to Customer Data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security.. Employees are granted access by role, and roles are reviewed at least once every six (6) months.

Background checks: All Datawarehouse.io employees undergo a third-party background check prior to being extended an employment offer, in accordance with and as permitted by the applicable laws. All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

1. **Transmission Control**

In-transit: We make HTTPS encryption (also referred to as SSL or TLS) available on every one of our login interfaces. Our HTTPS implementation uses industry standard algorithms and certificates.

At-rest: We store user passwords following policies that follow industry standard practices for security. We have implemented technologies to ensure that stored data is encrypted at rest.

1. **Input Control**

Detection: We designed our infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Datawarehouse.io personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: We maintain a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimize Integration and Subscriber damage or unauthorized disclosure. Notification to you will be in accordance with the terms of the DPA or Agreement.

1. **Availability Control**

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure.

Datawarehouse.io Integrations are designed to ensure redundancy and seamless failover. The server instances that support the Integrations are also architected with a goal to prevent single points of failure. This design assists our operations in maintaining and updating the Integration applications and backend while limiting downtime.

**Annex 3 - Sub-Processors**

This Annex forms part of the DPA.

To help us deliver the Integrations, we engage Sub-Processors to assist with our data Processing activities. A list of our Sub-Processors and our purpose for engaging them is located on our Sub-Processors page on our Site available at https://datawarehouse.io /subprocessors/. By agreeing to the DPA, you agree all of the Sub-Processors listed on our Site may have access to Customer Data.

**Appendix 1 to the Standard Contractual Clauses**

This Appendix forms part of the Standard Contractual Clauses.

A description of the Details of Processing, including (i) List of Parties, (ii) Description of the Transfer, and (iii) Competent Supervisory Authority are set out in Annex 1 of the DPA.

**DATA EXPORTER**

Name:

Authorized Signature

**DATA IMPORTER**

Name: James Elmer, Chief Technology Officer

 Authorized Signature

**Appendix 2 to the Standard Contractual Clauses**

This Appendix forms part of the Standard Contractual Clauses.

A description of the technical and organizational security measures implemented by the data importer in accordance with Standard Contractual Clauses are set out in Annex 2 of the DPA.

**DATA EXPORTER**

Name:

Authorized Signature

**DATA IMPORTER**

Name: James Elmer, Chief Technology Officer

 Authorized Signature

**Appendix 3 to the Standard Contractual Clauses**

This Appendix forms part of the Standard Contractual Clauses (the 'Clauses').

The List of Sub-Processors used by the data importer in accordance with Clause 9(a) of the Standard Contractual Clauses are set out in Annex 3 of the DPA:

**DATA EXPORTER**

Name:

Authorized Signature

**DATA IMPORTER**

Name: James Elmer, Chief Technology Officer

 Authorized Signature