NOTE:

The HighLevel Data Processing Agreement is made available on our website and is incorporated into the HighLevel Terms of Service available at *www.gohighlevel.com/terms-of-service*. For customers that would like to receive a signed copy of the HighLevel Data Processing Agreement, we have made this copy available to you. HighLevel does not accept any changes made to this copy.

Data Processing Agreement

VERSION APRIL 2023

This HighLevel Data Processing Agreement and its Annexes A, B, and C ("DPA") is between HighLevel Inc. ("HighLevel") and the party executing this agreement as Customer ("Customer"). This DPA reflects the parties' agreement with respect to the Processing of Personal Data by HighLevel on behalf of Customer in connection with the Service under the contemporaneously-executed Terms of Service agreement between the parties ("Agreement").

This DPA is part of the Agreement and is effective upon execution or another time as specified in the Agreement, an Order or an executed amendment to the Agreement. In case of any conflict or inconsistency with the terms of the Agreement, this DPA will take precedence over the terms of the Agreement to the extent of such conflict or inconsistency, and it will supersede any previous DPA.

1. Definitions

a. CCPA means California Civil Code Sec. 1798.100 et seq. as amended (also known as the California Consumer Privacy Act of 2018), including the California Privacy Rights Act amendments to the CCPA.

b. California Personal Information means Personal Data that is subject to the protection of the CCPA.

c. Controller, Processor, Data Subject, Personal Data, Personal Data Breach, Process, and Processing shall have the meaning given to them in the Data Protection Laws;

d. Customer Personal Data means any information relating to an identified or identifiable individual where (i) such information is contained within Customer Data provided under the Agreement; and (ii) is protected as personal data, personal information or personally identifiable information under applicable Data Protection Laws.

e. Data Protection Laws means all applicable worldwide legislation relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data in question under the Agreement, including without limitation, the European Data Protection Laws, the CCPA, and other US laws; in each case as amended, repealed, consolidated or replaced from time to time.

f. Europe means the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.

g. European Data means Personal Data that is subject to the protection of European Data Protection Laws.

h. 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, the GDPR; (ii) Directive 2002/58/EC concerning the Processing of personal data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); or (iii) GDPR as it forms parts of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR"); and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance ("Swiss DPA"); in each case, as may be amended, superseded or replaced.

i. GDPR means the General Data Protection Regulation ((*EU) 2016/679*), and the retained UK version of the same;

j. Standard Contractual Clauses means the standard contractual clauses annexed to the European Commission's Decision (EU) 2021/914 of 4 June 2021 currently found at https://ec.europa.eu/info/law/law-topic/data-

protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en, as may be amended, superseded or replaced;

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

2. Compliance. Both parties will comply with all applicable requirements of Data Protection Laws. This schedule is in addition to, and does not relieve, remove or replace, a party's obligations or rights under Data Protection Laws.

3. Controller/Processor. The parties have determined that for the purposes of Data Protection Laws, HighLevel shall process the Customer Personal Data as processor on behalf of the Customer. Customer may be either a Controller or Processor.

4. Consents. Customer will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of Customer Personal Data to HighLevel, and the lawful collection of the same by the Customer using the HighLevel Services for the duration and purposes of the Agreement and DPA, and shall indemnify HighLevel against all loss and damage (including fines) arising from a failure to do so.

5. Nature, Scope, Purpose of Processing, and Data Subjects. Annex A sets out the scope, nature, and purpose of Customer Personal Data Processing by HighLevel, the duration of the Processing and the types of Customer Personal Data and categories of Data Subjects.

6. Customer Instructions. HighLevel shall process Customer Personal Data only on the documented instructions of the Customer, unless HighLevel is required by any applicable laws to otherwise process that Customer Personal Data. The Agreement and DPA are deemed to be the instructions of Customer; the parties may agree to additional instructions. HighLevel shall inform the Customer if, in the opinion of HighLevel, the instructions of the Customer breach Data Protection Laws;

7. HighLevel Obligations. HighLevel will:

a. Implement and maintain appropriate technical and organizational measures to protect Customer Personal Data from Personal Data Breaches, as described under Annex B to this DPA ("Security Measures"). Notwithstanding any provision to the contrary, HighLevel may modify or update the Security Measures at HighLevel's discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures.

b. Ensure that any personnel engaged and authorised by HighLevel to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory or common law obligation of confidentiality;

c. Assist the Customer insofar as this is reasonably possible (taking into account the nature of the Processing and the information available to HighLevel), and at the Customer's cost and written request, in responding to any request from a Data Subject and in ensuring the Customer's compliance with its obligations under Data Protection Laws with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

d. Notify the Customer without undue delay on becoming aware of a Personal Data Breach involving the Customer Personal Data;

e. At the written direction of the Customer, delete or return Customer Personal Data and copies thereof to the Customer on termination of the Agreement unless HighLevel is required by any applicable law to continue to process that Customer Personal Data. For the purposes of this paragraph, Customer Personal Data shall be considered deleted where it is put beyond further use by HighLevel;

f. For European Data, assist Customer in ensuring compliance with Articles 32 to 36 of the GDPR; make available all information reasonably necessary to demonstrate compliance with this DPA available to Customer and allow for and reasonably contribute to audits, including inspections conducted by Customer to assess compliance with this DPA to the extent required by Data Protection Laws; and will make available all information reasonably necessary to demonstrate compliance with GDPR Article 28 requirements for Processors; and

g. Maintain records to demonstrate its compliance with this paragraph,

8. Service Provider. The parties agree that if the CCPA applies, Customer is a "business" and HighLevel is a "service provider" as defined under the CCPA. HighLevel will not retain, use, or disclose the California Personal Information it collects pursuant to the Agreement for any purposes other than to perform the Agreement or as otherwise permitted by the CCPA; and (b) HighLevel will not retain, use, or disclose the California Personal Information it collects pursuant to this the Agreement outside of the direct business relationship between HighLevel and Customer, unless otherwise permitted by the CCPA. HighLevel will not "sell" or "share" California Personal Information as those terms are defined in the CCPA or combine the California Personal Information with personal information obtained from sources other than Customer, except to the extent necessary to perform the Agreement. From time to time, Customer may ask for, and HighLevel will provide, reasonable evidence of its compliance with this Section 8.

9. Subprocessors. The Customer provides its prior, general authorization for HighLevel to appoint Processors to process the Customer Personal Data, provided that HighLevel shall ensure that the terms on which it appoints such processors comply with Data Protection Laws, and are consistent with the obligations imposed on HighLevel in this paragraph; and shall remain responsible for the acts and omission of any such Processor as if they were the acts and omissions of HighLevel. HighLevel has currently appointed, as Sub-Processors, the third parties listed in Annex C to this DPA. HighLevel will notify Customer if HighLevel adds or replaces any Sub-Processors listed in Annex C at least 30 days prior to any such changes, if Customer opts-in to receive such emails by contacting HighLevel. HighLevel will include substantially the same protections for Customer Personal Data as those in the DPA.

10. European Data: Transfer Mechanisms for Data Transfers/Standard Contractual Clauses.

a. HighLevel 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 European Data Protection Laws), unless it first takes all such measures as are necessary to ensure the transfer is in compliance with applicable European Data Protection Laws. Such measures may include (without limitation) transferring such Personal Data to a recipient that 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, to a recipient that has achieved binding corporate rules authorization in accordance with European Data Protection Laws, or to a recipient that has executed appropriate standard contractual clauses in each case as adopted or approved in accordance with applicable European Data Protection Laws.

b. Customer acknowledges that in connection with the performance of the Service, HighLevel is a recipient of European Data in the United States. Subject to sub-sections (c), 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) Customer is the "data exporter" and HighLevel is the "data importer"; (ii) the Module Two terms apply to the extent the Customer is a Controller of European Data and the Module Three terms apply to the extent the Customer is 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 the Republic of Ireland (without reference to conflicts of law principles); (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 in accordance with sub-section (1) 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 in accordance with sub-section (1) 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".

c. If HighLevel cannot comply with its obligations under the Standard Contractual Clauses or is breach of any warranties under the Standard Contractual Clauses or UK Addendum (as applicable) for any reason, and Customer intends to suspend the transfer of European Data to HighLevel or terminate the Standard Contractual Clauses, or UK Addendum, Customer agrees to provide HighLevel with reasonable notice to enable HighLevel to cure such non-compliance and reasonably cooperate with HighLevel to identify what additional safeguards, if any, may be implemented to remedy such non-compliance. If HighLevel has not or cannot cure the non-compliance, Customer may suspend or terminate the affected part of the Service in accordance with the Agreement without liability to either party (but without prejudice to any fees Customer have incurred prior to such suspension or termination).

11. Amendments. Notwithstanding anything else to the contrary in the Agreement, HighLevel reserves the right to make any updates and changes to this DPA, including to address changes in Data Protection Laws and to revise the security provisions in this DPA, so long as HighLevel does not materially reduce the overall security level provided to Customer Personal Data.

EXECUTED BY THE PARTIES' AUTHORIZED REPRESENTATIVES:

HIGHLEVEL INC.

DocuSigned by:

Signature: Robin Alex

F3FD86B65A8D4F6...

Printed Name: Robin Alex

Title: Co-Founder

Date: 4/7/2023

CUSTOMER:_____

Signature:_____

Printed Name:_____

Title:_____

Date:_____

ANNEX A - Details of Processing

A. List of Parties

Data exporter:

Name: You, as defined in HighLevel's Terms of Service

Address: Your address as specified by your Platform Account

Contact person's name, position and contact details: Your contact details, as specified by your Platform Account

Activities relevant to the data transferred under these Clauses: *Performance of the Agreement between the parties as a Controller.*

Role (controller/processor): *Controller or Processor*

Data importer:

Name: *HighLevel Inc.*

Address: *400 N. Saint Paul St. Suite 920, Dallas, Texas 75202, USA*

Contact person's name, position and contact details: *Robin Alex, Co-Founder*

Activities relevant to the data transferred under these Clauses: *Performance of the Agreement between the parties.*

Role (controller/processor): *Processor*

B. Description of Transfer

Categories of Data Subjects whose Personal Data is Transferred: *Customers and potential customers of clients.*

Categories of Personal Data Transferred: *The Personal Data input and collected as decided by the Customer, including name, age, date of birth, phone number, email address, social media profiles.*

Sensitive Data transferred and applied restrictions or safeguards: *The parties do not anticipate the transfer of sensitive data.*

Frequency of the transfer: *Variable during the Agreement term.*

Subject Matter and Nature of the Processing: *HighLevel will provide the Services to the Customer under the Agreement between the parties. The Customer will use the Services to collect and process Personal Data of their customers and potential customers for the purposes of managing and carrying out marketing activities, which may be targeted to their customers and potential customers.*

The Processing will involve collecting, storing, recording, contacting and managing Personal Data, in particular for the purpose of running marketing campaigns, providing marketing services, and managing marketing generally.

Purpose of the transfer and further Processing: *HighLevel will Process Personal Data as necessary to provide the Service pursuant to the Agreement, as further specified in an order form, and as further instructed by Customer in Customer's use of the Service.*

Period for which Personal Data will be retained: *The duration of the period in which the Customer accesses and uses the HighLevel platform under the Services Agreement.*

C. 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 Transfer Mechanisms for Data Transfers section of this DPA.

ANNEX B to the Standard Contractual Clauses

Description of the technical and organisational security measures implemented by the data importer in accordance with clause 4(d) and clause 5(c) (or documents/legislation attached):

Measure	Description
Measures of pseudonymisation and encryption of personal data	All personal data at rest is encrypted with: AES 256 CBC. All personal data in transit is encrypted with: TLS V1.2+.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Processor has endpoint protection on its APIs. Processor has uptime monitors to help ensure availability and to alert Processor if there is downtime. Processor has implemented access control measures such as user-based authentication and subaccount-base authentication. Processor uses managed services (AWS, GoogleCloud) to help ensure integrity.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Personal data backed up on AWS and GoogleCloud with 5 minute granularity to enable Processor to restore personal data in case of an incident.
Measures for user identification and authorisation	Processor uses encrypted signed tokens and role-based authorizations, as well as password protection.
Measures for the protection of data during transmission	SSL certificates and https are used during personal data transmission. Protected with TLS v1.2+.
Measures for the protection of data during storage	Personal data is encrypted at rest with AES-256 CBC encryption.
Measures for ensuring physical security of locations at which personal data are processed	Processor uses managed services to ensure physical security of server locations. All personal data stored on AWS and GoogleCloud, with physical security described in AWS and GoogleCloud Ts&Cs, respectively.
Measures for ensuring events logging	Processor uses logging for all user actions and audit logs. In particular, Processor uses GoogleCloud ops for both application and infrastructure monitoring. In addition, Processor uses AWS's Cloudwatch.
Measures for ensuring system configuration, including default configuration	Processor has configurations stored in version control. All containers are created from standardized images hosted by AWS and GoogleCloud. Updates and upgrades are performed automatically and managed by

	GoogleCloud. Patching of any vulnerabilities is managed by GoogleCloud, according to its standard policies.
Measures for internal IT and IT security governance and management	Processor uses a third-party vendor (iWerk) for internal IT and IT security.
Measures for certification/assurance of processes and products	The Compliancy Group has issued Processor a HIPAA Seal of Compliance Certificate.
Measures for ensuring data minimisation	Minimum data requirement set by Processor. Users can decide not to enter personal data into optional fields.
Measures for ensuring data quality	Processor enables customers to update relevant personal data to the latest date, and Processor uses two-factor authentication. Application monitoring conducted by GoogleCloud and custom monitors.
Measures for ensuring limited data retention	Data retention can be configured with respect to specific individuals by the customer administrator.
Measures for ensuring accountability	Processor access to personal data is restricted based on rules.
Measures for allowing data portability and ensuring erasure	Customers can download their personal data from within the Service. Customers can request a copy, or deletion, of their personal data upon separation Processor uses support tickets to ensure the foregoing.

Describe the specific technical and organisational measures to be taken by Data Importer to be able to provide assistance to the Data Exporter:

Measure	**Description**
Self-Service	Personal data can be downloaded by customers from within the Service. Customer admins can set data retention for terminated personnel.
Customer and Product Support	FAQs, support tickets for specific queries not addressed by collateral on Processor customer/product support website

ANNEX C – Subprocessors

Name of Authorized Subcontractor	**Address**	**Contact information**	**Description of processing**	**Country in which subprocessing will take place**
Google LLC/Google Cloud Services	1600 Amphitheatre Parkway, Mountain View, California 94043, United States	legal-notices@google.com	Data storage; support for performance of this Agreement	US
Amazon Web Services, Inc.	410 Terry Avenue North, Seattle, WA 98109-5210, United States	206.266.7010	Data storage; support for performance of this Agreement	US