# CUSTOMER DATA PROCESSING ADDENDUM

Last Updated: September 2025

This Customer Data Processing Addendum, including its exhibits and appendices (the "**Addendum**") is entered into between HighLevel, Inc., a corporation incorporated under the laws of Dallas, and its relevant Affiliates ("**HighLevel**"), and the counterparty accepting this Addendum ("**Customer**") (each, a "**Party**" and, collectively, the "**Parties**") by virtue of the Customer signing and accepting the Terms of Services Agreement (the "**Agreement**"). As of the effective date of the Agreement (the "**Effective Date**"), the terms of this Addendum shall be incorporated by reference and be part of the Agreement. In case of any conflict or inconsistency with the terms of the Agreement, this Addendum will take precedence over the terms of the Agreement to the extent of such conflict or inconsistency, and it will supersede any previous Addendum. For clarity, the Standard Contractual Clauses prevail over any other term of the Addendum terms. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended or supplemented by, and including, this Addendum.

## 1. Definitions.

1.1. For the purpose of interpreting this Addendum, the following terms (and their applicable cognates) shall have the meanings set out below:

(a) "**Account**" means any accounts or instances created by, or on behalf of, Customer or its Affiliates within the Services.

(b) "**Affiliate**" means any entity within a controlled group of companies that directly or indirectly, through one or more intermediaries, is controlling, controlled by, or under common control with one of the Parties.

(c) "**Applicable Data Protection Laws**" means all laws and regulations applicable to the Processing of Customer Personal Data, including but not limited to the laws and regulations identified in **Exhibit B** hereto as may be amended, modified, or supplemented from time to time, as applicable.

(d) "**Contracted Processor**" means any third party appointed by or on behalf of HighLevel to Process Customer Personal Data in connection with the Services.

(e) "**Customer Personal Data**" means Personal Data contained within Customer Data that HighLevel Processes by or on behalf of Customer to provide the Services in accordance with the Agreement. Customer Personal Data does not include Customer's Account information.

(f) "**Data Exporter**" and "**Data Importer**" shall have the same meanings assigned to them in **Part A of Exhibit A**.

(g) "**GDPR**" means the EU GDPR and UK GDPR as those terms are defined within **Exhibit B**, as applicable.

(h) "**Jurisdiction Specific Terms**" means all terms applicable to the Processing of Personal Data that apply to the extent that HighLevel Processes Customer Personal Data originating from, or protected by, Applicable Data Protection Laws in one of the jurisdictions identified in these terms. The Jurisdiction Specific Terms are currently available as **Exhibit B** to this Addendum and which may be moved online in accordance with Section 15 of this Addendum.

(i) "**Restricted Transfer**" means any transfer of Customer Personal Data protected by Applicable Data Protection Laws to a Third Country or an international organization in a Third Country (including data storage on foreign servers).

(j) "**SCCs**" or "**Standard Contractual Clauses**" are the model clauses for Restricted Transfers adopted from time to time by the relevant authorities of the jurisdictions indicated in **Exhibit B**, insofar as their use is approved by the relevant authorities as an appropriate mechanism or safeguard for Restricted Transfers.

(k) "**Services**" means the services and other activities carried out by or on behalf of HighLevel for Customer upon Customer's creation of an Account, whether through a free trial or paid subscription. For the avoidance of doubt, Services exclude services HighLevel performs as a Controller, such as managing customer relationships, account administration, and providing the areas of its website https://www.gohighlevel.com/ that can be accessed without creation of an Account.

(l) "**Sub-Processor**" means a direct Processor of a Processor. For the avoidance of doubt, Contracted Processors are Sub-Processors.

1.2. The terms "**Controller**", "**Data Protection Assessment**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Processor**", "**Rights of the Data Subjects**", "**Supervisory Authority**", and "**Third Country**" shall have the same meanings as under Applicable Data Protection Laws, and their cognate and corresponding terms shall be construed accordingly.

1.3. Capitalized terms which are used but not defined herein shall have the meanings given to them in the Agreement. Except as modified or supplemented above, the definitions of the Agreement shall remain in full force and effect.

**2. Scope and Applicability.**

2.1. Duration. This Addendum shall take effect on the Effective Date and shall continue concurrently for the duration that Personal Data is Processed by HighLevel pursuant to the Agreement.

2.2. Scope. This Addendum will apply to the Processing of all Customer Personal Data, regardless of country of origin, place of Processing, location of Data Subjects, or any other factor. The Processing of Personal Data that does not constitute Customer Personal Data is outside the scope of this Addendum.

2.3. Exhibits and Appendices. This Addendum includes the following exhibits and appendices:

(a) Exhibit A – Details of Processing;

(b) Appendix I to Exhibit A – Technical and Organizational Security Measures;

(c) Exhibit B – Jurisdiction Specific Terms; and

(d) Appendix I to Exhibit B – Supplemental Clauses to the Standard Contractual Clauses.

**3. Processing of Customer Personal Data.**

3.1. HighLevel will act as a Processor of Customer Personal Data. Customer will act as the Controller of Customer Personal Data. To the extent Customer acts as a Processor to other parties when processing Customer Personal Data, HighLevel will act as the Sub-Processor to Customer.

3.2. HighLevel shall:

(a) Comply with all Applicable Data Protection Laws in the Processing of Customer Personal Data;

(b) Not Process Customer Personal Data other than on Customer's relevant documented instructions, including to provide and improve the Services set forth in the Agreement (for clarity, such instructions include authorization to anonymize, deidentify, or aggregate Customer Personal Data and to provide HighLevel's AI features used for the Services), unless such Processing is permitted or required by Applicable Data Protection Laws; and

(c) immediately inform Customer in the event that, in HighLevel's reasonable opinion, a Processing instruction given by Customer may infringe Applicable Data Protection Laws.

3.3. All necessary information relating to the details of Processing is set out within **Exhibit A**.

3.4. Customer instructs HighLevel (and authorizes HighLevel to instruct each Contracted Processor it engages) to Process Customer Personal Data and, in particular, transfer Customer Personal Data to any country or territory, only as reasonably necessary for the provision of the Services and consistent with the Agreement and this Addendum.

**4. Personnel.** HighLevel shall take reasonable steps to ensure:

(a) the reliability of any employee, agent, or contractor who may have access to Customer Personal Data;

(b) that access to Customer Personal Data is strictly limited to those individuals who need to know or access it, as strictly necessary to fulfil the documented instructions given to HighLevel by Customer or to comply with Applicable Data Protection Laws; and

(c) that all such individuals are subject to formal confidentiality undertakings, professional obligations of confidentiality, or statutory obligations of confidentiality.

**5. Security of Processing.** HighLevel shall implement and maintain the administrative, technical, and organizational security measures identified within **Appendix I to Exhibit A**, which ensure a level of security appropriate to the risk of Processing and take into account: the state of the art, costs of implementation, and the nature and purposes of Processing; the risk of varying likelihood and severity to the rights and freedoms of natural persons; and the risks presented by the Processing activities, particularly those risks related to Personal Data Breaches.

**6. Contracted Processors.**

6.1. Authorization for Existing Contracted Processors: Customer authorizes HighLevel to continue using those Contracted Processors engaged as of the Effective Date and set out within HighLevel's website [https://www.gohighlevel.com/sub-processors], and further authorizes HighLevel and its Contracted Processors to appoint additional Contracted Processors, provided the obligations of this Section 6 (and the respective obligations of **Exhibit B**) are met.

6.2. Authorization for Appointment of Contracted Processors: To appoint an additional Contracted Processor, HighLevel will provide Customer with written notice, which will include the details of Processing to be undertaken as described within HighLevel's website. Customer may subscribe to receive such notifications by clicking "Click here to receive notifications of any updates to this list" at the following address: https://www.gohighlevel.com/sub-processors .

6.3. Objection to Contracted Processors:

(a) Customer will be deemed to have consented to the additional Contracted Processor if no objection is received within thirty (30) days of HighLevel's notice. Customer may object to the appointment of a Contracted Processor by providing a written objection, which

shall include the name of the objected-to Contracted Processor and a reasonable statement of objection.

(b) If an objection is received, the Parties will work together in good faith with a view of achieving a commercially reasonable resolution. If no mutually agreeable resolution is available, Customer may terminate the Agreement immediately upon written notice to HighLevel, with no further fees due, other than what has been accrued up to and including the date of termination. Upon notice of termination, HighLevel shall cease Processing Customer Personal Data.

6.4. Requirements for Appointing Contracted Processors: With respect to each Contracted Processor, HighLevel shall:

(a) restrict the Contracted Processor's access to Customer Personal Data only to what is necessary to assist HighLevel in providing the Services, and prohibit the Contracted Processor from accessing Customer Personal Data for any other purpose; and

(b) ensure that the arrangement between HighLevel and the Contracted Processor is governed by a written contract that includes terms which offer at least the same level of protection for Customer Personal Data as those set out in this Addendum, to the extent applicable to the nature of the services provided by such Contracted Processor.

6.5. Where any Contracted Processor fails to fulfil its data protection obligations under such written contract (or in the absence thereof, as the case may be), HighLevel shall remain fully liable to Customer for the performance of the respective Contracted Processors' data protection obligations under such contract and/or Applicable Data Protection Laws.

**7. Rights of the Data Subjects.**

7.1. Taking into account the nature of the Processing, HighLevel shall assist Customer by implementing appropriate technical and organizational measures, insofar as possible, to respond to valid requests to exercise Rights of the Data Subjects under Applicable Data Protection Laws.

7.2. With regard to the Rights of the Data Subjects within the scope of this Section 7, HighLevel shall:

(a) promptly notify Customer if it or any of its Contracted Processors receive a request from a Data Subject with respect to Customer Personal Data;

(b) not respond to that request, except on the documented instructions of Customer or as required by Applicable Data Protection Laws, in which case HighLevel shall, to the extent permitted by Applicable Data Protection Laws, inform Customer of such requirement before it responds to the request or directs its Contracted Processors to respond; and

(c) promptly comply with any documented instructions from Customer regarding responding to a request to exercise Rights of a Data Subject.

**8. Personal Data Breaches.**

8.1. Breach Response. If HighLevel discovers, is notified of, or has reason to suspect a Personal Data Breach affecting Customer Personal Data under its or its Contracted Processors' control, HighLevel will (i) immediately implement measures to stop the unauthorized access; (ii) secure the Customer Personal Data; and (iii) notify Customer without undue delay and, in any event, within seventy-two (72) hours of becoming aware of such suspected Personal Data Breach.

8.2. Breach Obligations. Immediately upon providing notice of a Personal Data Breach, HighLevel shall:

(a) describe to Customer in as much detail as reasonably possible: (i) the nature of the Personal Data Breach, (ii) where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned, (iii) the impact of such Personal Data Breach upon Customer and the affected Data Subjects, and (iv) the measures taken or proposed by HighLevel to address the Personal Data Breach;

(b) provide and supplement notifications as and when additional information becomes available;

(c) assist Customer in meeting its respective obligations pursuant to Applicable Data Protection Laws, including any obligations to notify Supervisory Authorities or Data Subjects of a Personal Data Breach; and

(d) use commercially reasonable efforts to investigate, mitigate, and remediate each such Personal Data Breach and prevent a recurrence of such Personal Data Breach.

8.3. No Acknowledgement of Fault. HighLevel's notification of or response to a Personal Data Breach under this Section will not be construed as an acknowledgement by HighLevel of any fault or liability with respect to the Personal Data Breach.

**9. Data Protection Assessment and Prior Consultation.** HighLevel shall provide Customer with relevant information and documentation, and assist Customer in complying with its obligations with regard to any data protection assessments or prior consultations with Supervisory Authorities when required pursuant to Applicable Data Protection Laws, but in each such case solely with regard to Customer Personal Data Processed by, and taking into account the nature of Processing and information available to, HighLevel and its Contracted Processors.

**10. Deletion or Return of Personal Data.**

10.1. HighLevel shall provide Customer with the technical means, consistent with the way the Services are provided, to request the deletion of Customer Personal Data, with the exception of any Customer Personal Data that may be retained pursuant to applicable laws.

10.2. If requested by Customer and following the cessation of Services, HighLevel shall promptly delete or return all Customer Personal Data (including copies) to Customer, with the exception of any Customer Personal Data that may be retained pursuant to applicable laws.

10.3. HighLevel shall also cause all Contracted Processors that have received Customer Personal Data to delete or return, as applicable, all such Customer Personal Data, with the exception of any Customer Personal Data that may be retained pursuant to applicable laws.

10.4. This Section 10 does not apply to Customer Personal Data that has been archived on back-up systems, which HighLevel or its Contracted Processors, as applicable, shall securely isolate and protect from any further Processing, except to the extent required by applicable law.

**11. Audit Rights.**

11.1. HighLevel shall allow for and contribute to audits, including remote inspections, by Customer or an auditor mandated by Customer (on behalf of itself or its clients) with regard to the Processing of the Customer Personal Data by HighLevel and its Contracted Processors. To the extent legally permitted, Customer shall reimburse HighLevel for any time expended for any such audit at HighLevel's then-current professional services rates, which shall be made available to Customer upon request.

12. **Jurisdiction Specific Terms.** To the extent HighLevel Processes Customer Personal Data originating from or protected by Applicable Data Protection Laws in a jurisdiction listed in **Exhibit B**, then the terms and definitions specified in **Exhibit B** with respect to the applicable jurisdiction shall apply in addition to the terms of this Addendum.

13. **Restricted Transfers.**

13.1. Restricted Transfers of Customer Personal Data within the scope of this Addendum shall be conducted in accordance with **Exhibit B** and Applicable Data Protection Laws.

13.2. If the relevant authorities adopt a new version of SCCs as a lawful mechanism for Restricted Transfers in a jurisdiction governing the processing of Customer Personal Data, the Parties are deemed to have agreed to the execution of the new version of the SCCs by signing this Addendum, and, if necessary, HighLevel shall be entitled to update **Exhibit A** and **Exhibit B** (and their appendices) accordingly.

13.3. If an alternative transfer mechanism, such as Binding Corporate Rules, is adopted by HighLevel during the term of the Agreement (an "**Alternative Mechanism**"), and HighLevel notifies Customer that some or all Restricted Transfers can be conducted in compliance with Applicable Data Protection Laws pursuant to the Alternative Mechanism, the Parties will rely on the Alternative Mechanism instead of the transfer mechanisms in **Exhibit B** for Restricted Transfers to which the Alternative Mechanism applies.

13.4. In addition, HighLevel is certified to the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework. HighLevel agrees to notify Customer if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Data Privacy Framework principles.

14. **No Selling of Customer Personal Data.** HighLevel acknowledges and confirms that it does not receive any Customer Personal Data as consideration for any Services or other items that HighLevel provides to Customer. As between Customer and HighLevel, Customer retains all rights and interests in Customer Personal Data. HighLevel agrees to refrain from taking any action that would cause any transfers of Customer Personal Data to or from HighLevel to qualify as selling Customer Personal Data under Applicable Data Protection Laws.

15. **Amendment and Online Hosting.**

15.1. Subject to the conditions specified in this Addendum, HighLevel may host the content of the exhibits and appendices of this Addendum online, and further update the Addendum / such exhibits and appendices, provided that prior notice is given to Customer.

(a) If no objection is received within fourteen (14) days of receipt of the notice, Customer will be deemed to have consented to the update. If Customer issues notice of non-acceptance, the Parties will cooperate and negotiate in good faith regarding any required updates.

(b) If no mutually agreeable resolution is available, Customer may terminate the Agreement immediately upon written notice to HighLevel, with no further fees due, other than what has been accrued up to and including the date of termination. Upon notice of termination, HighLevel shall cease Processing Customer Personal Data.

15.2. To the extent that the Addendum / an exhibit or appendix is hosted online, the latest version online shall take precedence over the relevant exhibit or appendix within this Addendum.

16. **Liability.**

16.1. Subject to Applicable Data Protection Laws, the liability of each Party under this Addendum shall be subject to the exclusions and limitations of liability set out in the Agreement.

**17. General Terms.**

17.1. Notice. The Parties shall use the Data Protection Contact provided in **Part A of Exhibit A** as contact points for all matters related to this Addendum, including notice of a Personal Data Breach and inquiries pursuant to Rights of the Data Subjects.

17.2. Prior Existing Agreement. This Addendum supersedes and replaces all prior and contemporaneous proposals, statements, sales materials or presentations, and agreements, oral and written, with regard to the subject matter of this Addendum, including any prior data processing addenda entered into between HighLevel and Customer in connection with the Agreement. Notwithstanding, all clauses of the Agreement that are not explicitly amended or supplemented by the clauses of this Addendum remain in full force and effect and shall apply, as long as this does not contradict compulsory requirements of Applicable Data Protection Laws.

17.3. Annual Review. Each Party must review this Addendum (including **Exhibit A** and its appendices) at regular intervals to ensure that the Addendum remains accurate, up to date, and continues to provide appropriate safeguards to the Personal Data. Each Party will carry out these reviews each time there is a change to the Personal Data, the purposes for Processing, the Data Importer information, or any risk assessments related to the Processing contemplated in this Addendum.

17.4. Conflicts. In the event of any conflict between the Agreement (including any annexures, exhibits, and appendices thereto) and this Addendum, the provisions of this Addendum shall prevail. In case of any conflict or ambiguity between the Jurisdiction Specific Terms and any other terms of this Addendum, the applicable Jurisdiction Specific Terms will prevail.

17.5. Severability. Should any provision of this Addendum be found legally invalid or unenforceable, then the invalid or unenforceable provision will be deemed superseded by a valid, enforceable provision that most closely matches the intent of the original provision, and the remainder of this Addendum will continue in effect.

17.6. Non-Compliance. If HighLevel determines that it can no longer meet any of its obligations set out within this Addendum, Applicable Data Protection Laws, or the SCCs (where applicable), it shall (i) promptly notify Customer of that determination and (ii) cease the Processing, if requested by Customer, or immediately take other reasonable and appropriate steps to remediate the lack of compliance.

17.7. Ambiguity. HighLevel may amend this Addendum without notice to or consent of Customer for the purposes of a) curing any ambiguity, b) curing, correcting or supplementing any defective provision contained herein, or c) making any other provisions with respect to matters or questions arising under this Addendum; provided that such action shall not materially alter the Addendum.

17.8. Signature. If you are accepting the terms of this Addendum on behalf of either Party, you represent and warrant that you have the authority to bind that Party and its Affiliates, where applicable, to the terms and conditions of this Addendum.

17.9. Disclosure to Supervisory Authorities. The Parties acknowledge that either Party may disclose this Addendum and any relevant privacy provisions in the Agreement to Supervisory Authorities, or any other judicial or regulatory body, upon their request.

**[ THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK ]**

**[ SIGNATURE PAGE TO THE CUSTOMER DATA PROCESSING ADDENDUM FOLLOWS ]**

Each Party is signing this Addendum on the date stated below that Party's signature.

| HighLevel, Inc. | [Customer's Full Legal Name] |
| --- | --- |
| Signature: Betsy Cantrell | Signature |
| Name: Betsy Cantrell | Name |
| Title: VP, Legal | Title |
| Date: 09 / 19 / 2025 | Date |

**[ SIGNATURE PAGE TO THE CUSTOMER DATA PROCESSING ADDENDUM ]**

# Exhibit A

**Details of Processing**

**A. LIST OF PARTIES:**

| | |
|---|---|
| **Name and Address:** | **HighLevel:**<br>HighLevel Inc. and its relevant Affiliates<br>5473 Blair Rd Ste 100, PMB 383313, Dallas, Texas 75231-4227<br><br>**Customer:**<br>Customer Name as defined in the HighLevel's Terms of Service and its relevant Affiliates<br>Customer address as specified by Customer's Platform Account. |
| **Data Protection Contact:** | **HighLevel:**<br>Betsy Cantrell - legal@gohighlevel.com<br>**Customer:**<br>Customer's contact details, as specified by Customer's Platform Account |
| **Activities Relevant to Transferred Data:** | Processing activities relating to the provision of the Services, as set forth in the Agreement. The Processing will involve collecting, storing, recording, contacting and managing Customer Personal Data, in particular for the purpose of running marketing campaigns, providing marketing services, and managing marketing generally. |
| **Controllership Role:** | *Customer as the Controller and HighLevel as the Processor:*<br>• To the extent Customer is the Controller of Customer Personal Data, HighLevel is Customer's Processor.<br>*Customer as the Processor and HighLevel as the Sub-Processor:*<br>• To the extent Customer is the Processor of Customer Personal Data, HighLevel is Customer's Sub-Processor. |
| **Data Transfer Role:** | **HighLevel:**<br>Data Importer |

| | |
|---|---|
| | **Customer:**<br><br>Data Exporter |

**B. DETAILS OF PROCESSING:**

| | |
|---|---|
| **Subject Matter of the Processing:** | The subject matter of the Processing of Customer Personal Data pertains to the provision of Services pursuant to the Agreement. |
| **Nature and Purpose of Processing:** | HighLevel will process Customer Personal Data as necessary to provide the Services under the Agreement, for the purposes specified in the Agreement and this Addendum, and in accordance with Customer's instructions as set forth in this Addendum. |
| **Retention Criteria (Duration):** | The duration of the period in which the Customer accesses and uses the HighLevel platform under the Services Agreement. |
| **Categories of Data Subjects:** | Customer may submit Personal Data as determined by Customer, which may include, but is not limited to, Personal Data relating to Customer, businesses and other entities contracting with Customer, and users of those businesses and other entities. |
| **Categories of Personal Data:** | As applicable, any Customer Personal Data that Customer provides into the Services. |
| **Special Categories of Personal Data:** | The Parties do not anticipate the transfer of special categories of data, unless Customer first notifies HighLevel in which case the Parties agree to apply appropriate restrictions and safeguards taking into consideration the nature of the data and the risks involved. |
| **Frequency of the Transfer:** | Regular and repeating for as long as Customer uses the Services. |
| **Subject Matter, Nature, and Duration of Contracted Processors:** | Same as above to the extent such information is provided to Contracted Processors for purposes of providing the Services. |

# Appendix I to Exhibit A

**Technical and Organizational Security Measures**

Throughout the term of the Agreement and for so long as HighLevel has access to any Customer Personal Data, HighLevel shall implement and maintain at least the following (or superior) technical and organizational security measures ("**TOMs**") to safeguard such Customer Personal Data:

| Type of TOMs | Description of TOMs |
|---|---|
| **Measures for pseudonymization 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:** | • The processor has endpoint protection on its user endpoint devices.<br>• Processor has uptime monitors to help ensure availability and to alert Processor if there is downtime.<br>• Processor has implemented access control measures such as role-based access control (RBAC) and subaccount-base authentication. The 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 five-minute granularity to enable Processor to restore personal data in case of an incident. |
| **Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure the security of the Processing:** | • Third party vulnerability scans or audits of externally facing infrastructure devices<br>• Annual third-party penetration testing of systems that store and process personal data.<br>• Maintain a standard patch management process and practice to ensure the protection of all devices used to access, process, or store personal data |
| **Measures for user identification and authorization:** | • Processor uses encrypted signed tokens and role-based authorizations, as well as password protection. |
| **Measures for the protection of Personal Data during transmission:** | • SSL certificates and https are used during personal data transmission. Protected with TLS v1.2+. |

| Type of TOMs | Description of TOMs |
|---|---|
| **Measures for the protection of Personal 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:** | • The 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:** | • The 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:** | • The 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:** | • The processor has an in-house team managing IT and IT Security and uses third-party MSSP for SOC monitoring. |
| **Measures for certification/assurance of processes and products:** | • The Compliancy Group has issued Processor a HIPAA Seal of Compliance Certificate. |
| **Measures for ensuring data minimization:** | • 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 role. |
| **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. |

| Type of TOMs | Description of TOMs |
|---|---|
| **Other:** | • Personal data can be downloaded by customers from within the Service. Customer admins can set data retention for terminated personnel.<br>• FAQs, support tickets for specific queries not addressed by collateral on Processor customer/product support website. |
| **Information about Contracted Processors' TOMs:** | Set forth in **Part B of Exhibit A**. |

# Exhibit B

**Jurisdiction Specific Terms**

1. **Australia.** When applicable, the Processing of Customer Personal Data shall be compliant with the Australian Privacy Principles, the Australian Privacy Act (1988), and any other applicable law, regulation, or decree of Australia pertaining to the protection of such information.

2. **Brazil.** Wherever the Processing pursuant to the Addendum falls within the scope of Brazil's Lei Geral de Proteção de Dados, Law No. 13.709 of 14 August 2018 and any other applicable law, regulation, or decree of Brazil pertaining to the protection of such information (collectively "**Brazilian Data Protection Laws**"), the provisions of the Addendum and this Section shall apply to such Processing.

   2.1. Restricted Transfers. With regard to any Restricted Transfer subject to Brazilian Data Protection Laws, one of the following transfer mechanisms shall apply, in the following order of precedence:

   (a) A valid adequacy decision adopted by the Brazilian Data Protection Authority ("**ANDP**") on the basis of Resolution 19/2024;

   (b) The Standard Contractual Clauses adopted by ANDP from time to time;

   (c) The recognition of a foreign Standard Contractual Clauses that provide an equivalent level of protection as the Brazilian Standard Contractual Clauses by the ANDP; or

   (d) Any other lawful data transfer mechanism, as laid down in Brazilian Data Protection Laws, as the case may be.

   2.2. Standard Contractual Clauses.

   (a) The Addendum hereby incorporates by reference the Brazilian Standard Contractual Clauses, including Section II in its entirety. The Parties are deemed to have accepted, executed, and signed the Brazilian Standard Contractual Clauses where necessary in their entirety.

   (b) The Parties agree that any references to clauses, and choices within the Brazilian Standard Contractual Clauses shall be deemed to be the same as the cognate and corresponding references within any appropriate, updated Standard Contractual Clauses as may be applicable from time to time pursuant to the Addendum.

   (c) For the purposes of the Brazilian Standard Contractual Clauses and any substantially similar Standard Contractual Clauses which may be adopted by the relevant authorities in the future, the Parties agree to apply the following:

      i. Clause 1: The content of Clause 1 is set forth in **Section A of Exhibit A** to the Addendum.

      ii. Clause 2: The content of Clause 2 is set forth in **Section B of Exhibit A** to the Addendum.

iii. Clause 3: The Parties choose Option B. The process for onward transfer is outlined Section 6 of the Addendum.

iv. Clause 4: The Parties choose Option A.

(A) Clause 4.1 (a): The Parties choose Exporter.

(B) Clause 4.1 (b): The Parties choose Exporter.

(C) Clause 4.1 (c): The Parties choose Exporter.

v. Section III: The content of Annex II is set forth in **Appendix I to Exhibit A** to the Addendum.

(d) In cases where the Brazilian Standard Contractual Clauses apply and there is a conflict between the terms of the Addendum and the terms of the Brazilian Standard Contractual Clauses, the terms of the Brazilian Standard Contractual Clauses shall prevail with regard to the Restricted Transfer in question.

**3. Canada.** When applicable, the Processing of Customer Personal Data shall be compliant with the Canadian Federal Personal Information Protection and Electronic Documents Act and any other applicable law, regulation, or decree of Canada pertaining to the protection of such information.

**4. European Economic Area.**

4.1. **Definitions.**

(a) "**EEA**" means the European Economic Area, consisting of the EU Member States, and Iceland, Liechtenstein, and Norway.

(b) "**EEA Data Protection Laws**" means the EU GDPR and all laws and regulations of the EU and the EEA countries applicable to the Processing of Customer Personal Data.

(c) "**EU 2021 SCCs**" means the contractual clauses adopted by the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

(d) "**EU GDPR**" (as used in the Addendum) means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, as may be amended from time to time.

4.2. **Restricted Transfers.**

(a) With regard to any Restricted Transfer subject to EEA Data Protection Laws between the Parties, one of the following transfer mechanisms shall apply, in the following order of precedence:

i. a valid adequacy decision adopted by the European Commission on the basis of Article 45 of the EU GDPR;

ii. the appropriate SCCs adopted by the European Commission from time to time; or

iii. any other lawful data transfer mechanism, as laid down in EEA Data Protection Laws.

**4.3. Standard Contractual Clauses.**

(a) The Addendum hereby incorporates by reference the SCCs. The Parties are deemed to have accepted, executed, and signed the SCCs where necessary in their entirety (including the annexures thereto).

(b) The Parties agree that any references to clauses, annexures, modules and choices within this Section shall be deemed to be the same as the cognate and corresponding references within any appropriate, updated SCCs as may be applicable from time to time pursuant to the Addendum.

(c) For the purposes of the EU 2021 SCCs and any substantially similar SCCs which may be adopted by the relevant authorities in the future:

i. the Parties agree to apply the following module:

(A) Module Two with respect to Controller-to-Processor Restricted Transfers; and

(B) Module Three with respect to Processor-to-Sub-Processor Restricted Transfers

ii. Clause 7: The Parties choose to include the optional docking clause;

iii. Clause 9(a): The Parties choose option 2, "General Written Authorization," and the time period set forth in Section 6.3 of the Addendum (The procedures for designation and notification of new Contracted Processors are set forth in more detail in Section 6 of the Addendum);

iv. Clause 11: The Parties choose not to include the optional language relating to the use of an independent dispute resolution body;

v. Clause 13 (Annex I.C): The competent Supervisory Authority is European Data Protection Board;

vi. Clause 17: The SCCs shall be governed by the laws of the Republic of Ireland;

vii. Clause 18: Any dispute arising from the SCCs shall be resolved by the courts of the Republic of Ireland;

viii. Annex I(A and B): The content of Annex I(A) and (B) is set forth in **Exhibit A**;

ix. Annex II: The content of Annex II is set forth in **Appendix I to Exhibit A.**

**(e)** The terms contained in **Exhibit C** to the Addendum supplement the SCCs.

**(f)** In cases where the SCCs apply and there is a conflict between the terms of the Addendum and the terms of the SCCs, the terms of the SCCs shall prevail with regard to the Restricted Transfer in question.

**10. Switzerland.**

**10.1. Definitions.**

**(a)** "**EU 2021 SCCs**" means the contractual clauses adopted by the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

**(b)** "**FDPIC**" means the Swiss Federal Data Protection and Information Commissioner.

(c) "**Swiss Data Protection Laws**" includes the Federal Act on Data Protection of 19 June 1992 ("**FADP**") and the Ordinance to the Federal Act on Data Protection.

10.2. **Restricted Transfers.**

(a) With regard to any Restricted Transfer subject to Swiss Data Protection Laws between the Parties, one of the following transfer mechanisms shall apply, in the following order of precedence:

i. a valid adequacy decision adopted by the FDPIC on the basis of Article 6 of the FADP;

ii. the appropriate SCCs adopted by the FDPIC from time to time; or

iii. any other lawful transfer mechanism, as laid down in Swiss Data Protection Laws.

**10.3. Standard Contractual Clauses.**

(a) The Addendum hereby incorporates by reference the EU 2021 SCCs, which have been adopted for use by the FDPIC with certain modifications. The Parties are deemed to have accepted, executed, and signed the EU 2021 SCCs where necessary in their entirety (including the annexures thereto).

(b) The Parties incorporate and adopt the EU 2021 SCCs for Restricted Transfers subject to Swiss Data Protection Laws in the same manner set forth in Section 7.3 of these Jurisdiction Specific Terms, subject to the following:

i. Clause 13 (Annex I.C): The competent authority shall be the FDPIC. Nothing about the Parties' designation of the competent Supervisory Authority shall be interpreted to preclude Data Subjects in Switzerland from applying to the FDPIC for relief;

ii. Clause 17: The SCCs shall be governed by the laws of Switzerland;

iii. Clause 18: Any dispute arising from the SCCs shall be resolved by the courts of Switzerland. The Parties' selection of forum may not be construed as forbidding Data Subjects habitually resident in Switzerland from suing for their rights in Switzerland;

iv. references to "Regulation (EU) 2016/679" and specific articles therein shall be replaced with references to the FADP and the equivalent articles or sections therein, insofar as there are any Restricted Transfers subject to Swiss Data Protection Laws; and

v. the SCCs also protect the data of legal entities until the entry into force of the revised FADP.

**(c)** In cases where the SCCs apply and there is a conflict between the terms of the Addendum and the terms of the SCCs, the terms of the SCCs shall prevail with regard to the Restricted Transfer in question.

**12. United Kingdom.**

**12.1. Definitions.**

(a) "**EU 2021 SCCs**" means the contractual clauses adopted by the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

(b) "**UK Data Protection Laws**" includes the Data Protection Act 2018 and the UK GDPR.

(c) "**UK GDPR**" (as used in the Addendum) means the United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

(d) "**UK ICO**" means the UK Information Commissioner's Office.

(e) "**UK Transfer Addendum**" (as used in this Section) means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued pursuant to Section 119A(1) of the Data Protection Act 2018 and approved by the UK Parliament.]

12.2. **Restricted Transfers.**

(a) With regard to any Restricted Transfer subject to UK Data Protection Laws between the Parties, one of the following transfer mechanisms shall apply, in the following order of precedence:

i. a valid adequacy decision adopted pursuant to Article 45 of the UK GDPR;

ii. the appropriate SCCs adopted by the UK ICO from time to time (insofar as the Processing activities of the Data Importer are not subject to the UK GDPR by virtue of application of Article 3(2) of the UK GDPR); or

iii. any other lawful data transfer mechanism, as laid down in the UK Data Protection Laws.

12.3. **EU 2021 SCCs and UK Transfer Addendum**.

(a) The Addendum hereby incorporates by reference the EU 2021 SCCs, which have been adopted for use by the UK ICO with certain modifications and the addition of the UK Transfer Addendum. The Parties are deemed to have accepted, executed, and signed the EU 2021 SCCs where necessary in their entirety (including the annexures thereto).

(b) For the purposes of the tables to the UK Transfer Addendum:

i. Table 1: The content of Table 1 is set forth in **Part A of Exhibit A**;

ii. Table 2: The content of Table 2 is incorporated and adopted as to Restricted Transfers subject to UK Data Protection Laws in exactly the same manner set forth in Section 7.3 of these Jurisdiction Specific Terms.;

iii. Table 3: The content of Table 3 (Annexes 1A, 1B, II, and III) is set forth as follows:

(A) *Annex 1*: The content of Annex 1 is set forth in **Exhibit A**;

(B) *Annex II*: The content of Annex II is set forth in **Appendix I to Exhibit A**; and

iv. Table 4: The Parties agree that neither Party may terminate the UK Transfer Addendum.

(c) The Parties incorporate and adopt the EU 2021 SCCs as to Restricted Transfers subject to UK Data Protection Laws in exactly the same manner set forth in Section 7.3 of these Jurisdiction Specific Terms, subject to the following:

i. Clause 13 (Annex I.C): The competent authority shall be UK ICO;

ii. Clause 17: The EU 2021 SCCs, including the incorporated UK Transfer Addendum, shall be governed by the laws of England and Wales; and

iii. Clause 18: Any dispute arising from the SCCs, or the incorporated UK Transfer Addendum, shall be resolved by the courts of England and Wales. A Data Subject may also bring legal proceedings against the Data Exporter and/or Data Importer

before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.

(d) The terms contained in **Exhibit C** to the Addendum supplements the SCCs.

(e) In cases where the SCCs, in conjunction with the UK Transfer Addendum, apply and there is a conflict between the terms of the Addendum and the terms of the SCCs or UK Transfer Addendum, the terms of the UK Transfer Addendum shall prevail with regard to the Restricted Transfer in question.

**13. United States of America.**

**13.1. Applicability.** Wherever the Processing pursuant to the Addendum falls within the scope of United States Data Protection Laws (defined below), the provisions of the Addendum and this Section shall apply to such Processing.

**13.2. Definitions.**

**(a)** "**United States Data Protection Laws**" include, individually and collectively, enacted state and federal laws, acts, and regulations of the United States of America that apply to the Processing of Personal Data, as may be amended from time to time. Such laws include, without limitation:

**i.** the California Consumer Privacy Act of 2018, as amended, including as amended by the California Privacy Rights Act of 2020 (Cal. Civ. Code § 1798.100 *et seq.*)., and the California Consumer Privacy Act Regulations, together with all implementing regulations;

**ii.** Similar state privacy laws, including, without limitation, the Colorado Privacy Act, the Connecticut Act Concerning Personal Data Privacy and Online Monitoring, the Delaware Personal Data Privacy Act, the Iowa Consumer Data Protection Act, the Maryland Online Data Privacy Act, the Minnesota Consumer Data Privacy Act, the Montana Consumer Data Privacy Act, the Nebraska Data Privacy Act, the New Hampshire Privacy Act, the New Jersey Senate Bill 332, the Oregon Consumer Privacy Act, the Tennessee Information Protection Act, the Texas Data Privacy and Security Act, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act.

(b) "**Personal Data Breach**" (as used in the Addendum) includes "Breach of Security" and "Breach of the Security of the System" as defined under applicable United States Data Protection Laws.

(c) The terms "**Business Purpose**", "**Commercial Purpose**", "**Sell**", and "**Share**" shall have the same meanings as under applicable United States Data Protection Laws, and their cognate and corresponding terms shall be construed accordingly.

13.3. **Processing of Customer Personal Data.**

**(a)** Customer discloses Customer Personal Data to HighLevel solely for: (i) valid Business Purposes; and (ii) to enable HighLevel to perform the Services.

**(b)** HighLevel shall not: (i) Sell or Share Customer Personal Data; (ii) retain, use or disclose Customer Personal Data except to provide the Services specified in the Agreement or as otherwise permitted by United States Data Protection Laws; or (iii) combine Customer Personal Data with other information that HighLevel Processes on behalf of other persons or that HighLevel collects directly from the Data Subject except as permitted by

United States Data Protection Laws. HighLevel certifies that it understands these prohibitions and agrees to comply with them.

13.4. **Termination.** Upon termination of the Agreement, HighLevel shall, as soon as reasonably practicable, destroy all Customer Personal Data it has Processed on behalf of Customer after the end of the provision of Services relating to the Processing and destroy all copies of the Customer Personal Data unless applicable law requires or permits storage of such Customer Personal Data.

# Appendix I to Exhibit B

**Supplemental Clauses to the Standard Contractual Clauses**

By this **Exhibit C** (this "**Exhibit**"), the Parties provide additional safeguards and redress to the Data Subjects whose Personal Data is transferred pursuant to SCCs. This Exhibit supplements and is made part of, but is not in variation or modification of, the SCCs that may be applicable to the Restricted Transfer.

1. **Definitions.** For the purpose of interpreting this Exhibit, the following terms shall have the meanings set out below:

   (a) "**EO 12333**" means the U.S. Executive Order 12333.

   (b) "**FISA**" means the U.S. Foreign Intelligence Surveillance Act.

   (c) "**Schrems II Judgment**" means the judgment of the European Court of Justice in Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems.

2. **Applicability of Surveillance Laws.**

   (a) Data Importer represents and warrants that, as of the Effective Date, it has not received any national security orders of the type described in Paragraphs 150-202 of the Schrems II judgment.

   (b) Data Importer represents that it reasonably believes that it is not eligible to be required to provide information, facilities, or assistance of any type under FISA Section 702 because:

      i. no court has found Data Importer to be an entity eligible to receive legal process issued under FISA Section 702: (i) an "electronic communication service provider" within the meaning of 50 U.S.C. § 1881(b)(4); or (ii) an entity belonging to any of the categories of entities described within that definition; and

      ii. if Data Importer were to be found eligible for process under FISA Section 702, which it believes it is not, it is nevertheless also not the type of provider that is eligible to be subject to UPSTREAM collection pursuant to FISA Section 702, as described in paragraphs 62 and 179 of the Schrems II judgment.

   (c) EO 12333 does not provide the U.S. government the ability to order or demand that Data Importer provide assistance for the bulk collection of information and Data Importer shall take no action pursuant to EO 12333.

3. **Backdoors.**

   3.1. Data Importer certifies that:

   (a) it has not purposefully created backdoors or similar programming for governmental agencies that could be used to access Data Importer's systems or Customer Personal Data subject to the SCCs;

   (b) it has not purposefully created or changed its business processes in a manner that facilitates governmental access to Customer Personal Data or systems; and

   (c) national law or government policy does not require Data Importer to create or maintain back doors or to facilitate access to Customer Personal Data or systems.

3.2. Data Exporter will be entitled to terminate the contract on short notice in cases in which Data Importer does not reveal the existence of a back door or similar programming or manipulated business processes or any requirement to implement any of these or fails to promptly inform Data Exporter once their existence comes to its knowledge.

4. **Information About Legal Prohibitions.** Data Importer will provide Data Exporter information about the legal prohibitions on Data Importer to provide information under this Exhibit. Data Importer may choose the means to provide this information.

5. **Additional Measures to Prevent Access.** Notwithstanding the application of the security measures set forth in the Addendum, Data Importer will implement internal policies establishing that:

   (a) Data Importer must require an official, signed document issued pursuant to the applicable laws of the requesting third party before it will consider a request for access to transferred Customer Personal Data;

   (b) Data Importer shall be notified upon receipt of each request or order for transferred Customer Personal Data;

   (c) Data Importer shall scrutinize every request for legal validity and, as part of that procedure, will reject any request Data Importer considers to be invalid;

   (d) if Data Importer is legally required to comply with an order, it will respond as narrowly as possible to the specific request; and

   (e) if Data Importer receives a request from public authorities to cooperate on a voluntary basis, Customer Personal Data transmitted in plain text may only be provided to public authorities with the express agreement of Data Exporter.

6. **Termination.** This Exhibit shall automatically terminate with respect to the Processing of Customer Personal Data transferred in reliance of the SCCs if the Supervisory Authority or a competent regulator approves a different transfer mechanism that would be applicable to the Restricted Transfers covered by the SCCs (and if such mechanism applies only to some of the data transfers, this Exhibit will terminate only with respect to those transfers) and that does not require the additional safeguards set forth in this Exhibit.

# Signature Certificate

Reference number: 52BA25E8-6303-4412-A344-DCD101E2C157

Sent on **September 18, 2025 10:10 PM UTC**

| Signed By | Signature |
| --- | --- |
| Betsy Cantrell<br>betsy@gohighlevel.com<br>Viewed: September 19, 2025 11:58 AM UTC<br>Signed: September 19, 2025 3:35 PM UTC |  <br>IP address: 50.53.209.12<br>Location: Beaverton, US |

Document completed by all parties on
September 19, 2025 3:35 PM UTC