DATA PROCESSING ADDENDUM

Last updated: Friday, July 5, 2024

This Data Processing Addendum and its appendixes ("**DPA**") form part of the Terms of Service available at www.hihello.com/legal/terms, or, if applicable, any other separate written agreement (the "**Agreement**" or "**Services Agreement**"), by and between HiHello, Inc., a Delaware corporation ("**HiHello**") and the Customer named in the Agreement, pursuant to which Customer has purchased a subscription to access and use the Service (as defined in the Agreement). The parties intend this DPA to be an extension of the Agreement governing certain requirements for HiHello's Processing of Personal Data provided or made available by Customer, or collected or otherwise obtained by HiHello, in the course of providing the Service to Customer. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between the terms of this DPA and the Agreement, the terms of this DPA shall prevail.

Customer enters into this DPA on behalf of itself and, to the extent required under Data Protection Legislation, in the name and on behalf of its Affiliates. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and such Affiliates.

1. Definitions.

1.1. "**Affiliate**" means any entity that is directly or indirectly controlled by, controlling or under common control with a party. "Control" for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.2. "**Controller**" means an entity that alone or jointly with others determines the purposes and means of Processing of Personal Data. For purposes of this DPA, a Controller includes a "business" as such term is defined by the CCPA, or a similar designation under Data Protection Legislation.

1.3. "**Data Privacy Framework**" or "**DPF**" means (as applicable) the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework and the UK Extension to the EU-U.S. Data Privacy Framework self-certification programs operated by the U.S. Department of Commerce, and their respective successors.

1.4. "**Data Privacy Framework Principles**" or "**DPF Principles**" means the Principles and Supplemental Principles contained in the relevant Data Privacy Framework, as amended, superseded or replaced.

1.5. "**Data Protection Legislation**" means European Data Protection Legislation and US Data Protection Legislation applicable to the processing of Personal Data under this DPA.

1.6. "**Europe**" means for the purposes of this DPA, the European Economic Area and/or its member states ("**EEA**"), the United Kingdom ("**UK**") and/or Switzerland.

1.7. "**European Data Protection Legislation**" means all data protection and privacy laws and regulations enacted in Europe and applicable (in whole or in part) to the respective party's Processing of Personal Data including (as applicable) (i) EU Regulation 2016/679 (General Data Protection Regulation) ("**EU GDPR**"); (ii) EU e-Privacy Directive (Directive 2002/58/EC), (iii) any national data protection laws made under or pursuant to (i) or (ii); (iv) in respect of the UK, the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"), the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003, and any other laws in force in the UK applicable to the Processing of Personal Data (together, "**UK Data Protection Legislation** "); and (v) the Swiss Federal Act on Data Protection of 2020 and its Ordinance ("**Swiss FADP**"); in each case as may be amended, superseded or replaced from time to time.

1.8. "**Personal Data**" means all information relating to an identified or identifiable natural person or consumer ("**Data Subject**"), including any data or information that is deemed "personal data", "personally identifiable information" and/or "personal information" under Data Protection Legislation.

1.9. "**Process**," "**Processes**," "**Processing**," "**Processed**" means any operation or set of operations which is performed on 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, destruction, or creating information from, Personal Data.

1.10. "**Processor**" means an entity that Processes Personal Data on behalf, and in accordance with the instructions, of a Controller. For purposes of this DPA, a Processor includes a "service provider" as such term is defined by the CCPA, or any similar or analogous designation under Data Protection Legislation.

1.11. "**Restricted Transfer**" means a transfer (directly or via onward transfer) of Personal Data that is subject to European Data Protection Legislation to a country outside Europe which is not subject to an adequacy determination by the European Commission, UK or Swiss authorities (as applicable).

1.12. "**Security Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise Processed by HiHello under this DPA. "Security Breach" shall not include unsuccessful attempts or activities that do not compromise the security of personal data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

1.13. "**Standard Contractual Clauses**" or "**SCCs**" shall mean the controller-to-processor contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021.

1.14. "**Subprocessor**" means any third party appointed by HiHello to Process Personal Data in connection with the provision of the Service. Subprocessors may include HiHello Affiliates but shall exclude HiHello employees, contractors, and consultants.

1.15. "**Supervisory Authority**" means any regulatory, supervisory, governmental, state agency, Attorney General or other competent authority with jurisdiction or oversight over compliance with Data Protection Legislation.

1.16. "**UK Addendum**" shall mean the International Data Transfer Addendum to the SCCs (version B1.0) issued by the Information Commissioner's Office under s.119(A) of the UK Data Protection Act 2018, as it is revised under Section 18 therein; as amended, superseded, or replaced from time to time.

1.17. "**US Data Protection Legislation**" means all privacy laws and regulations applicable in the United States, including the California Consumer Privacy Act, as amended by the California Privacy Rights Act, (the "**CCPA**"), as

well as any regulations and guidance issued thereunder; and, where applicable, (ii) the Virginia Consumer Data Protection Act ("**VCDPA**"); (iii) the Colorado Privacy Act ("**CPA**"); (iv) (v) the Connecticut Data Privacy Act ("**CTDPA**"); and the Utah Consumer Privacy Act when effective ("**UCPA**") when effective; in each case as may be amended or superseded from time to time.

2. **Scope.** The parties agree that, as between the parties, Customer is the Controller and that HiHello is the Processor in relation to the Personal Data that HiHello Processes on behalf of Customer in the course of providing the Service under the Services Agreement, as more particularly described in Appendix 1 of this DPA. The Processing will be carried out in accordance with this DPA until the date HiHello ceases to provide the Service to Customer.

3. **Data Protection.** In respect of Personal Data Processed in the course of providing the Service, HiHello shall adhere to the following requirements:

3.1. HiHello will Process the Personal Data (i) in accordance with the written instructions from Customer and only in compliance with Data Protection Legislation, and (ii) for the purposes described in Appendix 1, unless obligated to do otherwise by applicable law. If HiHello is required by law to Process the Personal Data for any other purpose, HiHello will inform Customer of such requirement prior to the Processing unless prohibited by law from doing so. The parties agree that the Agreement (including this DPA), and Customer's use of the Service in accordance with the Agreement, set out Customer's Processing instructions. Customer shall ensure its instructions are lawful and that the Processing of the Personal Data in accordance with such instructions will not violate Data Protection Legislation.

3.2. For the purposes of US Data Protection Legislation (to the extent applicable), HiHello shall not (a) sell or share Personal Data, as the term "sell" and "share" are defined by US Data Protection Legislation, (b) disclose or transfer Personal Data to a Subprocessor or any other parties that would constitute "selling" or "sharing" as these terms are defined by US Data Protection Legislation, (c) unless otherwise permitted by US Data Protection Legislation, retain, use, disclose, or otherwise Process the Personal Data for any purposes other than the purposes identified in Appendix 1 of this DPA, and (d) use Personal Data outside the direct relationship between Customer and HiHello or combine Personal Data received with Personal Data that HiHello receives from other sources or that it collects from its own interaction with the Data Subject, except as

otherwise directed by Customer or required to comply with Data Protection Legislation. HiHello agrees that Customer has the right to take reasonable and appropriate steps to help ensure that HiHello's use of Personal Data is consistent with Customer's obligations under US Data Protection Legislation.

3.3. HiHello will implement and maintain appropriate technical and organizational measures to protect the Personal Data against Security Breaches and preserve the security and confidentiality of Personal Data . Such measures shall include, at a minimum, those measures described in Appendix II ("**Security Measures**"). Customer acknowledges that the Security Measures are subject to technical progress and development and that HiHello may update or modify the Security Measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Service.

3.4. HiHello may engage Subprocessors to Process Personal Data on Customer's behalf and Customer hereby provides HiHello a general authorization to engage Subprocessors in order to provide the Service. HiHello will not engage new Subprocessors without giving Customer prior notice via an update to www.hihello.com/legal/subprocessors and a reasonable opportunity to object in good faith on data protection grounds, which, if not exercised within 30 days of such notice shall be deemed to constitute an approval of such engagement; notwithstanding the foregoing, the Subprocessors listed on www.hihello.com/legal/subprocessors ("**Subprocessors List**") as of the date of this DPA are deemed pre-approved by Customer, subject to the conditions contained herein. HiHello must include in any contract with Subprocessors provisions which ensure a level of protection for Personal Data that is substantially equivalent to those contained in this DPA and the Agreement. For the avoidance of doubt, where a Subprocessor fails to fulfill its obligations under any subprocessing agreement or Data Protection Legislation, HiHello will remain fully liable to Customer for the fulfillment of its obligations under this DPA and the Services Agreement.

3.5. HiHello will take reasonable steps to ensure the reliability and competence of any HiHello personnel who have access to the Personal Data. HiHello will ensure that all HiHello personnel required to access the Personal Data are informed of its confidential nature and comply with the obligations set out in this DPA.

3.6. HiHello will take all reasonable steps to assist Customer in meeting Customer's obligations under applicable Data Protection Legislation, including Customer's obligations to respond to requests by Data Subjects to exercise their rights with respect to Personal Data, adhere to data security obligations, respond to Security Breaches involving Personal Data, conduct data protection impact assessments, and consult with Supervisory Authorities. HiHello will promptly inform Customer in writing if it receives: (i) a request from a Data Subject concerning any Personal Data; or (ii) a complaint, communication, or request relating to Personal Data that HiHello Processes on behalf of Customer under the Agreement and this DPA. HiHello reserves the right to require reimbursement from Customer for the reasonable cost of any time, expenditures or fees incurred in connection with assistance provided at Customer's request to the extent permitted under Data Protection Legislation.

3.7. HiHello will not retain any of the Personal Data for longer than is necessary to provide the Service. At the end of the provision of the Service, unless indicated by Customer otherwise in writing, HiHello will securely destroy the Personal Data relating to the Processing. This later shall not apply to the extent HiHello is required by applicable law to retain some or all of the Personal Data, or to Personal Data archived on back-up systems, which data HiHello shall securely isolate and protect from any further Processing (to the extent permitted by applicable law).

3.8. HiHello shall provide written responses to all reasonable requests made by Customer for information relating to HiHello's Processing of Personal Data, including responses to information and security audit questionnaires submitted to it by Customer and that are necessary to confirm HiHello's compliance with this DPA, provided that Customer shall not exercise this right more than once per calendar year or when Customer is expressly requested or required to provide this information to a Supervisory Authority. While it is the parties' intention to ordinarily rely on the written responses described above to verify HiHello's compliance with this DPA and Data Protection Legislation, following a confirmed Security Breach or where a Supervisory Authority requires it, Customer may provide HiHello with thirty (30) days' prior written notice requesting that a third-party conduct an audit of HiHello's facilities, equipment, documents and electronic data relating to the Processing of Personal Data under the Agreement ("**Audit**"), provided that: (a) the Audit shall be conducted at Customer's expense; (b) the parties shall mutually agree upon the scope, timing and duration of the Audit; and (c) the Audit shall

not unreasonably impact HiHello's regular operations. Customer acknowledges that any written responses or Audit shall be subject to the confidentiality provisions of the Agreement.

3.9. If HiHello becomes aware of a Security Breach affecting Personal Data that is Processed by HiHello in the course of providing the Service under the Agreement:

3.9.1. it shall within 72 hours and without undue delay notify Customer and provide Customer with: a detailed description of the Security Breach; the type of data that was the subject of the Security Breach; and the steps HiHello has or will take in order to mitigate and remediate such Security Breach, in each case as soon as such information can be collected or otherwise becomes available (as well as periodic updates to this information and any other information Customer may reasonably request relating to the Security Breach); and

3.9.2. take reasonable steps to contain, investigate and mitigate the effects of the Security Breach and to identify, prevent and mitigate the effects of the Security Breach and, with the prior written approval of Customer, to carry out any recovery or other action necessary to remedy the Security Breach.

3.10. HiHello will notify Customer immediately if, in HiHello's reasonable opinion, an instruction for the Processing of Personal Data given by Customer infringes applicable Data Protection Legislation.

4. Data Transfers.

4.1. HiHello as data exporter.

4.1.1. Subject to complying with the terms of this Section 4.1, Customer acknowledges and agrees that HiHello may transfer or disclose Personal Data to and in the United States and other locations in which HiHello or its Subprocessors maintain Processing operations (as more particularly described in the Subprocessors List).

4.1.2. HiHello shall at all times ensure that such transfers, including Restricted Transfers, are made in compliance with the requirements of Data Protection Legislation and this DPA. If HiHello engages in a Restricted Transfer, such measures may include (without limitation) transferring the Personal 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, including the DPF; (ii) has achieved binding corporate rules authorization; or (iii) has executed SCCs; in each case as adopted or approved in accordance with Data Protection Legislation.

4.2. HiHello as data importer. The parties agree that, when the transfer of Personal Data from Customer to HiHello is a Restricted Transfer, HiHello shall comply with the following:

4.2.1. Data Privacy Framework: HiHello shall use the DPF to lawfully receive Personal Data in the United States and HiHello shall ensure that it provides at least the same level of protection to such Personal Data as is required by the DPF Principles.

4.2.2. SCCs: If the DPF does not cover the Restricted Transfer and/or it is invalidated, the SCCs shall automatically be incorporated into this DPA and apply to the Restricted Transfers as follows:

a) EU Transfers: In relation to Personal Data that is protected by the EU GDPR, the SCCs will apply completed as follows:

i. Module Two (Controller to Processor) will apply;

ii. in Clause 7, the optional docking clause will not apply;

iii. in Clause 9, Option 2 will apply, and the time period for prior notice of Subprocessor changes shall be as set out in Section 3.3 of this DPA;

iv. in Clause 11, the optional language will not apply;

v. in Clause 17, Option 1 will apply, and the SCCs will be governed by the laws of the Republic of Ireland;

vi. in Clause 18(b), disputes shall be resolved before the courts of the Republic of Ireland;

vii. Annex I of the SCCs shall be deemed completed with the information set out in Appendix 1 of this DPA; and

viii. Annex II of the SCCs shall be deemed completed with the information set out in Appendix 2 of this DPA.

b) UK Transfers: In relation to Personal Data that is protected by UK Data Protection Legislation, the SCCs: (i) shall apply as completed in accordance paragraph a.(i)-(viii) above; and (ii) shall be deemed amended as specified by the UK Addendum, which shall deemed executed by the parties and incorporated into and form an integral part of this DPA. In addition, Tables 1 to 3 in Part 1 of the UK Addendum shall be completed respectively with the information set out in Appendixes 1 and 2 of this DPA and Table 4 in Part 1 shall be deemed completed by selecting "neither party".

c) Swiss Transfers: In relation to Personal Data that is protected by the Swiss FADP, the SCCs will apply in accordance with paragraph a.(i)-(viii) above with the following modifications:

i. references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss FADP;

ii. references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss FADP;

iii. references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland" or "Swiss law";

iv. the term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., Switzerland);

v. Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the Swiss Federal Data Protection Information Commissioner;

vi. references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection

Information Commissioner" and "applicable courts of Switzerland";

vii. in Clause 17, the SCCs shall be governed by the laws of Switzerland; and

viii. Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland.

d) It is not the intention of either party to contradict or restrict any of the provisions set forth in the SCCs and, accordingly, if and to the extent the SCCs conflict with any provision of the Agreement (including this DPA) the SCCs shall prevail to the extent of such conflict.

5. **Customer Responsibilities**. Customer is responsible for determining whether the Service is appropriate for the storage and Processing of Personal Data under Data Protection Legislation. Customer further agrees that: (a) it will comply with its obligations under Data Protection Legislation regarding its use of the Service and the Processing of Personal Data; (b) it has provided notice and obtained all consents, permissions and rights necessary for HiHello and its Subprocessors to lawfully Process Personal Data for the purposes contemplated by the Agreement (including this DPA); and (c) it will notify HiHello if it is unable to comply with its obligations under Data Protection Legislation or if its Processing instructions will cause HiHello or its Subprocessors to be in breach of Data Protection Legislation.

6. **Limitation of liability**. Any claim or remedy Customer or its Affiliates may have against HiHello, its employees, agents and Subprocessors, arising under or in connection with this DPA (including the Standard Contractual Clauses), whether in contract, tort (including negligence) or under any other theory of liability, shall to the maximum extent permitted by law be subject to the limitations and exclusions of liability in the Agreement. Accordingly, any reference in the Agreement to the liability of a party means the aggregate liability of that party and all of its Affiliates under and in connection with the Agreement and this DPA together.

7. **Permitted Disclosures**. Each party acknowledges that the other party may disclose the SCCs, this DPA and any privacy related provisions in the Agreement to any European or US regulator upon request.

8. **Governing Law and Jurisdiction**. This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the

Agreement, unless required otherwise by Data Protection Legislation or the SCCs.

Appendix 1: Description of Processing Activities/ Transfer

This Appendix 1 forms part of the DPA and describes the Processing that HiHello (as the Processor) will perform on behalf of Customer (as the Controller).

Annex I (A): List of Parties	
Data Exporter	**Data Importer**
Name: [Customer Name as provided to HiHello] ("**Customer**")	**Name:** HiHello, Inc. ("**HiHello**")
Address: [Customer Address as provided to HiHello]	**Address:** 927 Industrial Ave, Palo Alto, CA 94303, United States
Contact Person's Name, position and contact details: [Customer Contact person as provided to HiHello]	**Contact Person's Name, position and contact details:** privacy@hihello.com
Activities relevant to the transfer: See Appendix 1 (B) below.	**Activities relevant to the transfer:** See Appendix 1 (B) below.
Signature and date: This Appendix 1 I shall automatically be deemed executed when the Agreement is executed by Customer.	**Signature and date:** This Appendix 1 shall automatically be deemed executed when the Agreement is executed by HiHello.
Role: Controller	**Role:** Processor

Annex I (B): Description of transfer	
Description of Transfer	**Categories of Data Subjects whose Personal Data is transferred**: The categories of Data Subjects will depend upon Customer's use of the Service as set out in the Agreement. To the extent the transfer contains Personal Data, it may concern: - Employees of Customer - Individual contacts of Customer, including, but not limited to, current and potential customers, clients, partners, prospects, and attendees of events hosted or sponsored by Customer - any other data subjects whose personal data may be processed from time to time pursuant to the Agreement and this DPA **Categories of Personal Data transferred**: The Personal Data that will be included in the transfer will depend upon Customer's use of the Service as set out in the

	Agreement. To the extent the transfer contains Personal Data, it may consist of: - Photographs and/or video of data subjects - Full or partial name (including but not limited to prefix, first name, middle name, last name, suffix, maiden name) - Accreditations - Preferred name and pronouns - Audio and phonetic pronunciation - Title, department, company, and headline message - Email address(es) - Telephone number(s) - Address(es) - Website links - PDF documents - Social media profiles like LinkedIn, Facebook, Instagram, X , and more - Important dates - IP address - Any other information the Customer or the Data Subject chooses to include on the Data Subject's HiHello digital business card **Sensitive Data Transferred (if appropriate) and applied Restrictions or Safeguards**: HiHello does not want to, nor does it intentionally, collect or process any Sensitive Data in connection with the provision of the Service. No sensitive data is intended to be transferred unless the user includes it unexpectedly in unstructured data. **Frequency of the Transfer (e.g. whether the data is transferred on a one-off or continuous basis)**: Continuous

	Purpose of the Data Transfer/Processing Operations: HiHello shall only process Customer Data for the Permitted Purposes, which shall include: (i) processing as necessary to provide the Service in accordance with the Agreement; (ii) processing initiated by Customer in its use of the Service; and (iii) processing to comply with any other reasonable instructions provided by Customer (e.g., via email or support tickets) that are consistent with the terms of the Agreement. **Nature and subject matter of the processing:** The provision of the Service to Customer as set out in the Agreement. HiHello is a software-as-a-service platform for digital brand and identity that enables individuals and companies of all sizes to leverage digital business cards, email signatures, and virtual backgrounds to present their brand consistently in every interaction, whether that is in-person, on video, or over email. HiHello offers applications that are available on the Web, on iOS, and Android. The HiHello platform allows users to share their digital business card, and also allows them to optionally receive their contact information in return. **Duration of the processing:** The duration of the Processing under the DPA is until the termination of the Agreement in accordance with its terms, plus the period from the expiry of the Agreement until deletion of Personal Data in accordance with the terms of the Agreement and this DPA. **Period for which the Personal Data will be retained, or if that is not possible the criteria used to determinate that period, if applicable**: As above.
Annex I (C): Competent Supervisory Authority	
Competent Supervisory Authority	The competent supervisory authority will be determined in accordance with Data Protection Legislation.

Appendix 2: HiHello's Technical And Organisational Security Measures

HiHello adopts an Information Security Management Systems (ISMS) as a framework for continuous improvement of security.

This ISMS includes (but is not limited to):

Policies

HiHello has and periodic reviews the Information Security Policies as the major guidelines for security practices. This includes Risk Management, Data Classification, Access Control, Software Development and Data Breaches.

Awareness

Awareness on security and compliance is fundamental and provided to all users. Some users may have additional specific awareness, relevant for their function.

Access control

Access is granted on a need-to-know basis and only a small number of users can access production systems where information from Customers is stored. Authentication to production systems is made with 2-factor Authentication as a standard.

Audit logging

Relevant audit logs are maintained, including access to sensitive information (including personal data). The logs are kept in separate infrastructure and only accessed by Security team.

Data Breaches

Processes are defined to handle Data Breaches. These processes include notification to relevant stakeholders, according to type of incident and applicable legislation.

Network security

HiHello implemented several security measures to protect our infrastructure from external and internal threats. This includes encryption, firewalls, IDS and other cloud provider specific. Access to production systems is made in secure mode and encryption in transit is a default. Sensitive information is also encrypted at rest.

Physical Security

HiHello uses data centers managed by cloud providers and delegates all physical security to them, after a due diligence.

Business Continuity

HiHello has several technical implementations to assure business continuity of its service. Those include backups, resilient and redundant infrastructure and a Disaster Recovery Plan.

Development

Development is made using a secure development methodology that includes peer review and secure coding and testing.

Continuous improvement and review

HiHello security posture is based on a continuous improvement process that includes periodic review of security controls effectiveness.