

DATA PROCESSING ADDENDUM

Bobyard, Inc., a corporation with a principal place of business located at 455 Market St Ste 1940 PMB 173694, San Francisco, CA 94105 ("**Company**") and the Bobyard customer whose name and principal place of business are set forth in Schedule 2, Annex 1 hereto ("**Customer**") enter into this Data Processing Addendum (including the Schedules and Annexes attached hereto, together "**DPA**") as of the date signed by both parties. This DPA forms part of the SaaS Subscription Agreement (collectively, the "**Agreement**") between the parties under which Company will provide the Service(s) to Customer which involves the Processing of Personal Data subject to Applicable Data Protection Laws (each as defined below). The purpose of this DPA is to set forth the terms under which Company Processes Personal Data on behalf of Customer.

This DPA consists of the main body and Schedules 1 through 4. Execution of this DPA shall constitute execution of the Standard Contractual Clauses and their Annexes as set forth in Schedules 1 and 2).

- 1. Definitions.** Capitalized terms used but not defined in this DPA have the meanings set forth in the Agreement. The terms controller, data subject, processor and supervisory authority have the meanings set forth in the Applicable Data Protection Laws.
- a. "**Authorized Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity, where "control" refers to the power to direct or cause the direction of the subject entity, whether through ownership of voting securities, by contract or otherwise.
 - b. "**Applicable Data Protection Laws**" means the privacy, data protection and data security laws and regulations of any jurisdiction applicable to the Processing of Personal Data under the Agreement, including, without limitation, European Data Protection Laws, UK GDPR and the United States including the CCPA.
 - c. "**CCPA**" means the California Consumer Privacy Act of 2018 and any regulations promulgated thereunder, in each case, as amended from time to time, including the California Privacy Rights Act of 2020, and any regulations promulgated thereunder.
 - d. "**EEA**" means the European Economic Area.
 - e. "**European Data Protection Laws**" means the GDPR and other data protection laws and regulations of the EEA and European Union, and the Member States of each of the foregoing, to the extent applicable to the Processing of Personal Data under the Agreement.
 - f. "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
 - g. "**Information Security Incident**" means a confirmed breach of Company's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in Company's possession, custody or control. Information Security Incidents do 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, or other network attacks on firewalls or networked systems.
 - h. "**Personal Data**" means Customer Data that constitutes "personal data," "personal information," or "personally identifiable information" defined in Applicable Data Protection Laws, or information of a similar character regulated thereby," provided that such data is electronic data and information submitted by or for Customer to the Services.
 - i. "**Processing**" or "**Process**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,

dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- j. **"Public Authority"** means a government agency or law enforcement authority, including judicial authorities.
- k. **"Security Measures"** are Company's security measures implemented and maintained as administrative, technical and physical safeguards designed to protect the security and integrity of Personal Data and prevent Information Security Incidents, further described in Schedule 2 Annex II hereto and any other measures required by Applicable Data Protection Laws.
- l. **"Standard Contractual Clauses"** means Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, currently located here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj and as amended from time to time due to changes in Applicable Data Protection Law.
- m. **"Subprocessors"** or **"Sub-processor"** means any third party processor that Company engages to Process Personal Data in relation to the Services.
- n. **"UK GDPR"** means the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("**UK GDPR**") and the Data Protection Act 2019.

2. **Duration and Scope of DPA.** This DPA will remain in effect so long as Company Processes Personal Data, notwithstanding the expiration or termination of the Agreement. Schedules 1 and 2 to this DPA apply solely to Processing subject to European Data Protection Laws. Schedule 3 to this DPA applies solely to Processing subject to the UK GDPR. Schedule 4 to this DPA applies solely to Processing subject to the CCPA to the extent Customer is a "business" (as defined in CCPA) with respect to such Processing.

3. **Customer Instructions.** Company will Process Personal Data only in accordance with Customer's instructions to Company. This DPA is a complete expression of such instructions, and Customer's additional instructions will be binding on Company only pursuant to an amendment to this DPA signed by both parties. Customer instructs Company to Process Personal Data via the Services and as authorized by the Agreement. Company shall inform Customer immediately: (a) if, in its opinion, an instruction from Customer constitutes a breach of any Applicable Data Protection Laws; (b) if Company is unable to follow Customer's instructions for the Processing of Personal Data; or (c) if Company has reason to believe that Company is subject to changes in Applicable Data Protection Laws contrary to any Customer instructions or terms or requirements of this DPA.

4. **Security of Personal Data.**

- a. **Company Security Measures.** Company may update the Security Measures from time to time, so long as the updated measures do not materially decrease the overall protection of Personal Data.
- b. **Information Security Incidents.** Company will notify Customer without undue delay of any Information Security Incident of which Company becomes aware. Such notifications will describe available details of the Information Security Incident, including steps taken to mitigate the potential risks and steps Company recommends the Customer take to address the Information Security Incident. Company's notification of or response to an Information Security Incident will not be construed as Company's acknowledgement of any fault or liability with respect to the Information Security Incident

5. **Audits of Compliance & DPIAs.** Company shall maintain an audit program to help ensure compliance with the obligations set out in this DPA and shall make available to Client information to demonstrate compliance with the obligations set out in this DPA, including those obligations required by applicable Data Protection Laws, as set forth in this section 5.

- a. **Third-Party Certifications and Audits.** Company agrees to maintain an information security program for the Services that complies with the standards defined within each of our certifications. Upon Client's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Company shall make available to Client that is not a competitor of Company (or Client's independent, third-party auditor that is not a competitor of Company) a copy of Company's then most recent third-party audits or certifications, as

applicable. Such third-party audits or certifications may also be shared with Client's competent supervisory authority on its request. Upon request, Company shall also provide a requesting Client with a report and/or confirmation of Company's audits of third-party Sub-processors' compliance with the data protection controls set forth in this DPA and/or a report of third-party auditors' audits of third party Sub-processors that have been provided by those third-party Sub-processors to Company, to the extent such reports or evidence may be shared with Client ("Third-party Sub-processor Audit Reports"). Client acknowledges that (i) Third-party Sub-processor Audit Reports shall be considered Confidential Information as well as confidential information of the third-party Sub-processor and (ii) certain third-party Sub-processors to Company may require Client to execute a non-disclosure agreement with them in order to view a Third-party Sub-processor Audit Report.

- b. **On-Site Audit.** Client may contact Company to request an on-site audit of Company's Processing activities covered by this DPA ("On-Site Audit"). An On-Site Audit may be conducted by Client either itself or through a Third-Party Auditor (as defined below in section 5(d)) selected by Client when:
 - (i) the information available pursuant to section "Third-Party Certifications and Audits" is not sufficient to demonstrate compliance with the obligations set out in this DPA and its Schedules;
 - (ii) Client has received a notice from Company of a Client Data Incident; or
 - (iii) such an audit is required by Data Protection Laws or by Client's competent supervisory authority. Any On-Site Audits will be limited to Client Data Processing and storage facilities operated by Company or any of Company's Affiliates. Client acknowledges that Company operates a multi-tenant cloud environment. Accordingly, Company shall have the right to reasonably adapt the scope of any On-Site Audit to avoid or mitigate risks with respect to, and including, service levels, availability, and confidentiality of other Company customers' information.
- c. **Reasonable Exercise of Rights.** An On-Site Audit shall be conducted by Client or its Third-Party Auditor:
 - (i) acting reasonably, in good faith, and in a proportional manner, considering the nature and complexity of the Services used by Client;
 - (ii) up to one time per year with at least three weeks' advance written notice. If an emergency justifies a shorter notice period, Company will use good faith efforts to accommodate the On-Site Audit request; and
 - (iii) during Company's normal business hours, under reasonable duration and shall not unreasonably interfere with Company's day-to-day operations. Before any On-Site Audit commences, Client and Company shall mutually agree upon the scope, timing, and duration of the audit and the reimbursement rate for which Client shall be responsible. All reimbursement rates shall be reasonable, considering the resources expended by or on behalf of Company.
- d. **Third-Party Auditor.** A Third Party Auditor means a third-party independent contractor that is not a competitor of Company. An On-Site Audit can be conducted through a Third Party Auditor if: (i) prior to the On-Site Audit, the Third Party Auditor enters into a non-disclosure agreement containing confidentiality provisions no less protective than those set forth in the Agreement to protect Company's proprietary information; and (ii) the costs of the Third Party Auditor are at Client's expense.
- e. **Findings.** Client must promptly provide Company with information regarding any non-compliance discovered during the course of an On-Site Audit.
- f. **Data Protection Impact Assessments (DPIAs).** Upon Customer's written request, Company will provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under Applicable Data Protection Laws to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Company.

6. Customer's Responsibilities.

- a. Customer Obligations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal

Data and the means by which Customer acquired Personal Data. Customer specifically acknowledges and agrees that its use of the Services will not violate the rights of any data subject, including those that have opted-out from sales or other disclosures of personal data, to the extent applicable under Applicable Data Protection Laws. Without limitation of Customer's obligations under the Agreement, Customer: (a) agrees that Customer is solely responsible for its use of the Services, including (1) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Personal Data, (2) securing the account authentication credentials, systems and devices Customer uses to access the Services, (3) securing Customer's systems and devices that Company uses to provide the Services, and (4) backing up Personal Data; and (b) has given all notices to, and has obtained all consents from, including where the Customer is a processor by ensuring that the ultimate controller does so, individuals to whom Personal Data pertains and all other parties as required by applicable laws or regulations for Company to Process Personal Data as contemplated by the Agreement.

- b. Prohibited Data. Customer represents and warrants to Company that Customer Data does not and will not, without Company's prior written consent, contain any social security numbers or other government-issued identification numbers, protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA) or other information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; health insurance information; biometric information; passwords for online accounts; credentials to any financial accounts; tax return data; credit reports or consumer reports; any payment card information subject to the Payment Card Industry Data Security Standard; information subject to the Gramm-Leach-Bliley Act, Fair Credit Reporting Act or the regulations promulgated under either such law; information subject to restrictions under Applicable Data Protection Laws governing Personal Data of children, including, without limitation, all information about children under 16 years of age; or any information that falls within any special categories of data (as defined in GDPR).

7. Compliance with Laws

- a. Compliance with Laws. Each party will comply with all Applicable Data Protection Laws, and for clarity with respect to GDPR and/or UK GDPR as provided for in Schedules 1 through 3 hereto. In particular, Customer will comply with its obligations as controller (or on behalf of controller) and Company will comply with its obligations as processor.
- b. Changes in Applicable Data Protection Laws. Company shall use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services, to facilitate compliance with changes in Applicable Data Protection Laws without unreasonably burdening Customer. If Company is unable to make available necessary changes promptly, Customer may terminate the applicable Order Form(s) and suspend the transfer of Personal Data in respect only to those Services which cannot be provided by Company in accordance with the changes in Applicable Data Laws by providing written notice in accordance with the "Notices" section of the Agreement. Customer shall receive a refund of any prepaid fees for the period following the effective date of termination for such terminated Services

8. Data Requests

- a. Personal Data Disclosures & Government Requests. Company will not disclose Personal Data to any third party, including any Public Authority, except: (i) as otherwise permitted under the Agreement including this DPA; or (ii) as necessary to comply with Applicable Data Protection Laws including with respect to any valid and/or binding Public Authority court order (e.g., a law enforcement subpoena). If Company receives a binding order from a Public Authority requesting access to or disclosure of Personal Data, Company will notify Customer of the request unless otherwise legally prohibited.
- b. Data Subject Request Assistance. Company will (considering the nature of the Processing of Personal Data) provide Customer with assistance reasonably necessary for Customer to perform its obligations under Applicable Data Protection Laws to fulfill requests by data subjects to exercise their rights under Applicable Data Protection Laws ("**Data Subject Requests**") with respect to Personal Data in Company's possession or control. Where permitted under Applicable Data Protection Laws, Customer will compensate Company for any such assistance at Company's then-current professional services rates, which will be made available to Customer upon request.

- c. Customer's Responsibility for Requests. Company will not respond to a Data Subject Request itself, except where Customer authorizes Company to redirect the Data Subject Request as necessary to allow Customer to respond directly. If Company receives a Data Subject Request, Company will advise the data subject to submit the request to Customer and Customer will be responsible for responding to the request.

10. Subprocessors.

- a. Consent to Subprocessor Engagement. Customer authorizes the following Subprocessors to Process Personal Data: (i) Company's Affiliates; and (ii) the Subprocessors set forth in Schedule 2 Annex III hereto, as updated by Company from time to time, or such other website address as Company may provide to Customer from time to time) ("**Subprocessor Site**").
- b. Requirements for Subprocessor Engagement. When engaging any Subprocessor, Company will enter into a written contract with such Subprocessor containing data protection obligations not less protective than those in this DPA with respect to Personal Data to the extent applicable to the nature of the services provided by such Subprocessor. Company shall be liable for all obligations under the Agreement subcontracted to, the Subprocessor or its actions and omissions related thereto.
- c. Subprocessor Changes. When Company engages any new Subprocessor after the Effective Date of the Agreement, Company will provide Customer with at least fifteen (15) days' prior notice. This Section 10(c) will not apply with respect to GDPR but instead will be replaced by the requirements of the Standard Contractual Clauses set forth in Section 4(g) and 4(h) of Schedule 1 hereto.
- d. Opportunity to Object to Subprocessor Changes. If Customer objects to such engagement in a written notice to Company on reasonable grounds relating to the protection of Personal Data within thirty (30) days of notice of the changes, Customer and Company will work together in good faith to find a mutually acceptable resolution to address such objection. If the parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, Customer may, as its sole and exclusive remedy, terminate the Agreement by providing written notice to Company.

- 11. Return or Deletion of Personal Data.** Upon request by Customer made within 30 days after the effective date of termination or expiration of this Agreement, Company will make Customer Data available to Customer for export or download as provided in the Documentation. After such 30-day period, Company will have no obligation to maintain or provide any Customer Data.

- 12. Miscellaneous.** Except as expressly modified by the DPA, the terms of the Agreement remain in full force and effect. In the event of any conflict or inconsistency between this DPA and the other terms of the Agreement, this DPA will govern. Notwithstanding anything in the Agreement or any order form entered in connection therewith to the contrary, the parties acknowledge and agree that Company's access to Personal Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement. Notwithstanding anything to the contrary in the Agreement, any notices required or permitted to be given by Company to Customer under this DPA may be given: (a) in accordance with any notice clause of the Agreement; (b) to Company's primary points of contact with Customer; or (c) to any email provided by Customer for the purpose of providing it with Services-related communications or alerts. Customer is solely responsible for ensuring that such email addresses are valid.

IN WITNESS WHEREOF, the undersigned have executed this Agreement by their duly authorized representatives, with the intention to be legally bound.

CUSTOMER: _____

BOBYARD, INC.

By: _____

By: Michael Ding

Name: _____

Name: Michael Ding

Title: _____

Date: _____

Title: **CEO** _____

Date: **10/82026** _____

SCHEDULE 1

TRANSFER MECHANISMS FOR STANDARD CONTRACTUAL CLAUSES DATA TRANSFERS

1. **Definitions.** For the purposes of Schedules 1 and 2, these terms shall be defined as follows:
 - a. **"EU C-to-P Transfer Clauses"** means Standard Contractual Clauses sections I, II, III and IV (as applicable) to the extent they reference Module Two (Controller-to-Processor).
 - b. **"EU P-to-P Transfer Clauses"** means Standard Contractual Clauses sections I, II, III and IV (as applicable) to the extent they reference Module Three (Processor-to-Processor).
2. **International Transfer Mechanisms.** If, in the performance of the Services, Personal Data that is subject to GDPR, or any other law relating to the protection or privacy of individuals under European Data Protection Laws, is transferred to countries which do not ensure an adequate level of data protection within the meaning of the European Data Protection Laws, the transfer mechanisms listed below shall apply to such transfers and can be directly enforced by the parties to the extent such transfers are subject to the European Data Protection Laws:
 - a. **The EU C-to-P Transfer Clauses.** Where Customer and/or its Authorized Affiliate is a Controller and a data exporter of Personal Data and Company is a Processor and data importer in respect of that Personal Data, then the parties shall comply with the EU C-to-P Transfer Clauses, subject to the additional terms in Schedule 1; and/or
 - b. **The EU P-to-P Transfer Clauses.** Where Customer and/or its Authorized Affiliate is a Processor acting on behalf of a Controller and a data exporter of Personal Data and Company is a Processor and data importer in respect of that Personal Data, the parties shall comply with the terms of the EU P-to-P Transfer Clauses, subject to the additional terms in Schedule 1.
3. **Roles.** For the purposes of the EU C-to-P Transfer Clauses and the EU P-to-P Transfer Clauses, Customer is the data exporter and Company is the data importer and the parties agree to the following. If and to the extent an Authorized Affiliate relies on the EU C-to-P Transfer Clauses or the EU P-to-P Transfer Clauses for the transfer of Personal Data, any references to Customer in this Schedule includes such Authorized Affiliate. Where this Schedule 1 does not explicitly mention EU C-to-P Transfer Clauses or EU P-to-P Transfer Clauses it applies to both of them.
4. **Standard Contractual Clauses Operative Provisions and Additional Terms.**
 - a. **Reference to the Standard Contractual Clauses.** The relevant provisions contained in the Standard Contractual Clauses are incorporated by reference and are an integral part of this DPA. The information required for the purposes of the Annexes to the Standard Contractual Clauses are set out in Schedule 2.
 - b. **Docking Clause.** The option under clause 7 shall not apply.
 - c. **Instructions.** This DPA and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement to Company for the Processing of Personal Data. Any additional or alternate instructions must be consistent with the terms of this DPA and the Agreement. For the purposes of clause 8.1(a), the instructions by Customer to Process Personal Data include onward transfers to a third party located outside the EEA for the purpose of the performance of the Services.
 - d. **Certification of Deletion.** The parties agree that the certification of deletion of Personal Data that is described in clauses 8.5 and 16(d) of the Standard Contractual Clauses shall be provided by Company to Customer only upon Customer's written request.
 - e. **Security of Processing.** For the purposes of clause 8.6(a), Customer is solely responsible for making an independent determination as to whether the technical and organisational measures set forth herein meet Customer's requirements and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of its Personal Data as well as the risks to individuals) the security measures and policies implemented and maintained by Company provide a level of security appropriate to the risk with respect to its Personal Data. For the purposes of clause 8.6(c), personal data

breaches (i.e., Information Security Incidents) will be handled in accordance with Section 4(b) of this DPA.

- f. Audits of the SCCs. The parties agree that the audits described in clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with Section 5 of this DPA.
- g. General Authorization for Use of Subprocessors. Option 2 under clause 9 shall apply. The data importer has the data exporter's general authorization for the engagement of Subprocessor(s) from those set forth in Annex III (see Schedule 2 below). The data importer shall inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors. The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

Where Company enters into the EU P-to-P Transfer Clauses with a Subprocessor in connection with the provision of the Services, Customer hereby grants Company and Company's Affiliates authority to provide a general authorization on Controller's behalf for the engagement of subprocessors by Subprocessors engaged in the provision of the Services, as well as decision making and approval authority for the addition or replacement of any such subprocessors.

- h. Notification of New Subprocessors and Objection Right. Pursuant to clause 9(a), Customer acknowledges and expressly agrees that Company may engage new Subprocessors as described in Section 4(g) above. Company shall inform Customer of any changes to Subprocessors following the procedure provided for in Section 4(g) above. Customer may object to new Subprocessors as described in Section 10(c) of the DPA.
- i. Redress. The option under clause 11 shall not apply. Company shall inform Customer if it receives a Data Subject Request with respect to Personal Data and shall without undue delay communicate the complaint or dispute to Customer. Company shall not otherwise have any obligation to handle the request (unless otherwise agreed with Customer).
- j. Liability. Company's liability under clause 12(b) shall be limited to any damage caused by its Processing where Company has not complied with its obligations under the GDPR specifically directed to Processors, or where it has acted outside of or contrary to lawful instructions of Customer, as specified in Article 82 GDPR.
- k. Supervision. Clause 13 shall apply as follows:
 - i. Where Customer is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by Customer with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.
 - ii. Where Customer is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority.
 - iii. Where Customer is established in the United Kingdom or falls within the territorial scope of application of UK GDPR, the Information Commissioner's Office shall act as competent supervisory authority.
- l. Notification of Government Access Requests. For the purposes of clause 15(1)(a), Company shall notify Customer (only) and not the Data Subject(s) in case of government access requests. Customer shall be solely responsible for promptly notifying the Data Subject as necessary.
- m. Governing Law. The governing law for the purposes of clause 17 shall be the law that is designated in the section of the Agreement. If the Agreement is not governed by an EU Member State law, the Standard Contractual Clauses will be governed by either: (i) the laws of Ireland; or (ii) where the Agreement is governed by the laws of the United Kingdom, the laws of the United Kingdom.
- n. Choice of Forum and Jurisdiction. The courts under clause 18 shall be those designated in the Agreement. If the Agreement does not designate an EU Member State court as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with this Agreement, the parties agree that the courts of either: (i) Ireland; or (ii) where the Agreement designates the United Kingdom as having exclusive jurisdiction, the United

Kingdom, shall have exclusive jurisdiction to resolve any dispute arising from the Standard Contractual Clauses.

- o. Data Exports from the United Kingdom under the Standard Contractual Clauses. In case of any transfers of Personal Data from the United Kingdom subject exclusively to the UK GDPR, except where such Processing is subject to Schedule 3 hereto: (i) general and specific references in the Standard Contractual Clauses to GDPR or EU or Member State Law shall have the same meaning as the equivalent reference in the Applicable Data Protection Laws of the United Kingdom (i.e., UK GDPR); and (ii) any other obligation in the Standard Contractual Clauses determined by the Member State in which the data exporter or Data Subject is established shall refer to an obligation under UK GDPR.
 - p. Conflict. The Standard Contractual Clauses are subject to this DPA and the additional safeguards set out hereunder. The rights and obligations afforded by the Standard Contractual Clauses will be exercised in accordance with this DPA, unless stated otherwise. In the event of any conflict or inconsistency between the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.
5. Additional Terms for the EU P-to-P Transfer Clauses. For the purposes of the EU P-to-P Transfer Clauses (only), the parties agree the following:
- a. Instructions and notifications. For the purposes of clause 8.1(a), Customer hereby informs Company that it acts as Processor under the instructions of the relevant Controller in respect of Personal Data. Customer warrants that its Processing instructions as set out in the Agreement and this DPA, including its authorizations to Company for the appointment of Subprocessors in accordance with this DPA, have been authorized by the relevant Controller. Customer shall be solely responsible for forwarding any notifications received from Company to the relevant Controller where appropriate.
 - b. Security of Processing. For the purposes of clause 8.6(c) and (d), Company shall provide notification of a personal data breach (i.e., an Information Security Incident) concerning Personal Data Processed by Company to Customer.
 - c. Documentation and Compliance. For the purposes of clause 8.9, all enquiries from the relevant Controller shall be provided to Company by Customer. If Company receives an enquiry directly from a Controller, it shall forward the enquiry to Customer and Customer shall be solely responsible for responding to any such enquiry from the relevant Controller where appropriate.
 - d. Data Subject Rights. For the purposes of clause 10 and subject to section 9(b) of this DPA, Company shall notify Customer about any request it has received directly from a Data Subject without obligation to handle it (unless otherwise agreed) but shall not notify the relevant Controller. Customer shall be solely responsible for cooperating with the relevant Controller in fulfilling the relevant obligations to respond to any such request.

SCHEDULE 2

ANNEX I THROUGH III TO THE STANDARD CONTRACTUAL CLAUSES

This Schedule 2 contains Annex I through III to the Standard Contractual Clauses and must be completed and signed by each party below where indicated.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): *Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*

Name: Customer

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses: Performance of the Services under the Agreement and as further described in the Documentation

Signature and date: _____

Role: For the purposes of SCC Module 2 Customer is a Controller. For the purposes of SCC Module 3 Customer is a Processor

Data importer(s): *Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*

Name: Bobbyard Inc.

Address: Bobbyard Inc, 455 Market St Ste 1940 PMB 173694, San Francisco, California 94105-2448 US

Contact person's name, position and contact details: JJ Shultz, Head of Engineering, jj@bobyard.com

Activities relevant to the data transferred under these Clauses: Performance of the Services under the Agreement and as further described in the Documentation

Signature: _____

B. DESCRIPTION OF THE TRANSFER

The Processing activities carried out by Company under the Agreement may be described as follows:

Categories of data subjects whose personal data is transferred

- Customer's Authorized Users, including employees, contractors, and agents of Customer who access or use the Services on Customer's behalf.
- Customer's end customers and prospective end customers who are natural persons, such as homeowners, property owners, and other individuals who engage Customer for contracting,

landscaping, or design services.

- Employees and contact persons of Customer's end customers and prospective end customers that are legal entities, such as developers, general contractors, property managers, and commercial property owners.
- Other individuals whose personal data appears in project materials Customer submits to the Services, including architects, engineers, designers, subcontractors, suppliers, and occupants of the relevant properties.

Categories of personal data transferred

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Property and project location data, including addresses of properties associated with identified or identifiable individuals.
- Personal data contained in project materials Customer submits to the Services, to the extent such materials identify or relate to an identifiable individual.
- Project and transaction data relating to individuals, associated with an identified or identifiable end customer.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No sensitive personal data is intended to be transferred or required for the provision of the Services.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous basis depending on the use of the Services by Customer.

Nature of the processing

The nature of the Processing is the performance of the Services under the Agreement.

Purpose(s) of the data transfer and further processing

Bobyard will Process Personal Data as necessary to perform the Services under the Agreement, as further specified in the Documentation, and as further instructed by Customer in its use of the Services.

The duration of the period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Subject to section 11 of the DPA, Bobyard will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority in accordance with Clause 13 of the Standard Contractual Clauses as identified in Schedule 1 Section 4(k) of this DPA.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Company will, as a minimum, implement the following technical and organizational measures designed to secure the Personal Data Vendor processes as part of its Services:

1. Access control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

- authenticated application access w/ role base permissions
- infrastructure account controls
- application apis require authenticated access by default, using django rest framework authentication
- password controls include django password validators for similarity, minimum length, common-password rejection, and numeric-password rejection, plus registration-time minimum and maximum password length validation.
- access to critical infrastructure and corporate systems is protected with mfa through gcp, aws, and heroku. Company also uses session, csrf, and authentication middleware, and rate limiting is implemented for selected unauthenticated endpoints.
- https/tls for internet-facing application traffic and requires ssl for production database connections.
- production secrets and service credentials are managed through environment-based configuration. application logging and change tracking support monitoring and investigation of suspicious access

2. Data access control

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, include:

- Internal policies and procedures
- Control authorization schemes
- Differentiated access rights (profiles, roles, transactions and objects), granted on “least-privilege” principle
- Validation of credentialed CORS configurations
- authenticated application access
- role-based authorization
- company and project-level scoping

Operationally, Bobbyard also uses controls to support least-privilege access and auditability. All production systems (Heroku, AWS, and GCP) require MFA.

3. Disclosure control

Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, include:

- Encryption/Tunneling
- Logging
- Transport security

4. Entry control

Technical and organizational measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, include:

- Logging and reporting systems
- Audit trails and documentation

5. Control of instructions

Technical and organizational measures to ensure that Personal Data are processed solely in accordance with the instructions of Subscriber include:

- Unambiguous wording of the contract
- Formal commissioning (request form)
- Criteria for selecting the Processor

6. Availability control

Technical and organizational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical) include:

- Backup procedures
- Mirroring of hard disks (e.g. RAID technology) or other applicable technology for local storage redundancy
- Uninterruptible power supply (UPS)- as provided by our Cloud provider (more information here: <https://www.google.com/about/datacenters/data-security/>)
- Remote storage
- Anti-malware/firewall systems
- Disaster recovery plan

7. Separation control

Technical and organizational measures to ensure that Personal Data collected for different purposes can be processed separately include:

- Separation of databases
- “Internal client” concept / limitation of use
- Segregation of functions (production/testing)
- Procedures for storage, amendment, deletion, transmission of data for different purposes

8. Business Continuity and Disaster Recovery

Vendor utilizes a cloud hosting provider, the AWS Platform, for all system infrastructure. Because of this, both Vendor and its clients benefit from AWS policies and practices as part of the data centers' DNA. The platform is built on custom-build servers exclusively for the data centers, never selling or distributing them outside of AWS premises. AWS has robust disaster recovery measures in place. For example, in the event of a fire or any other disruption, data access shifts automatically and seamlessly to another data center so that the users can keep working, uninterrupted. There are emergency backup generators, which continue to power the data centers even in the event of a power failure. AWS is responsible for maintaining the physical security of all servers.

9. Customer Data Portability and Deletion

Upon request by Customer made within 30 days after the effective date of termination or expiration of the Agreement, Vendor will make Customer Data available to Customer for export or download as provided in the Documentation. After such 30-day period, Vendor will have no obligation to maintain or provide any Customer Data.

ANNEX III

LIST OF SUB-PROCESSORS

The Controller has authorized the use of the Subprocessors identified with their locations at <https://www.bobyard.com/legal/data-processing-addendum/#subprocessors>.

SCHEDULE 3

TRANSFER MECHANISMS FOR UK GDPR

- A. **Definitions.** For the purposes of this Schedule 3, these terms shall be defined as follows:
- a. **“UK GDPR IDTA”** means the terms of the “International Data Transfer Agreement” (located here: <https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf>) and issued pursuant to Section 119A of the Data Protection Act 2018.
 - b. **“UK GDPR Addendum”** or **“UK Addendum”** means the terms of the “International Data Transfer Addendum to the European Commission’s Standard Contractual Clauses for International Data Transfers” (located here: <https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf>) and issued pursuant to Section 119A of the Data Protection Act 2018.
- B. **International Transfer Mechanisms.** If, in the performance of the Services, Personal Data that is subject to UK GDPR or any other law relating to the protection or privacy of individuals that applies in the United Kingdom is transferred out of the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of the European Data Protection Laws, the UK GDPR IDTA and/or UK Addendum shall apply to such transfers and can be directly enforced by the Parties to the extent such transfers are subject to the UK GDPR.
- C. **Appendix Information.** Annex I through III, set forth in Schedule 2 to this DPA, contain Appendix Information for the UK IDTA and UK Addendum and are incorporated therein by reference.

SCHEDULE 4

UNITED STATES SCHEDULE

- A. The parties acknowledge that Customer discloses Personal Data to Company for the limited and specified purposes set forth in the Agreement and DPA, and as instructed by Customer.
- B. Customer shall have the right to take the reasonable and appropriate steps set forth in the Agreement designed to stop and remediate unauthorized use of Personal Data.
- C. Company will not retain, use, disclose, sell, or share the Personal Data other than providing the Services specified by Customer's documented instructions. Company will not combine Personal Data with information received from, or on behalf of other entities, except to perform the purpose of providing the Services specified by Customer's documented instructions. Company shall Process Personal Data in accordance with Data Protection Laws applicable to Company's provision of the Services to its customers generally (i.e., without regard for Customer's particular use of the Services), when the Services are used according to this DPA, the Agreement, the Documentation, and the applicable Order Form. Company shall inform Customer if Company determines it is unable to meet its obligations under the CCPA.
- D. The parties acknowledge that Company's retention, use and disclosure of personal information authorized by Customer's instructions documented in the DPA are integral to Company's provision of the Services and the business relationship between the parties.