redesign

DATA PROCESSING AGREEMENT

Version Date: September 2026

This Data Processing Agreement ("DPA") is hereby incorporated into and governed by the Terms and Conditions located at https://www.redesign-group.com/legal (the "Agreement") between The Drala Project, Inc. d/b/a The Redesign Group ("Redesign") and Customer and applies to the extent that Redesign processes Personal Data (as defined herein) on behalf of Customer in the performance of Services thereunder. The purpose of this DPA is to set out the rights and obligations of the Parties in respect of the Personal Data processed by Redesign in its capacity as a processor or service provider under the Agreement.

I. Definitions

a) "Controller," "business," "processor," "service provider," "data subject," "consumer," "process," "sale," "sell," "business purpose," and "supervisory authority" (or any equivalent terms) have the meaning set out under Data Protection Laws.

b) "AI Act" means Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (the EU Artificial Intelligence Act), as amended or superseded from time to time.

c) "Canadian Privacy Laws" means the Personal Information Protection and Electronic Documents Act ("PIPEDA") and substantially similar provincial legislation, including the Province of Quebec's Act respecting the protection of personal information in the private sector, as amended by Law 25.

d) "European Data Protection Laws" means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as amended or superseded from time to time ("EU GDPR"); the EU GDPR as it forms part of the law of the United Kingdom by virtue of section 3 of the UK European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018, in each case as amended by the Data (Use and Access) Act 2025 (together, "UK Data Protection Laws"); and the Swiss Federal Act on Data Protection of 25 September 2020 (FADP, SR 235.1) and its implementing Ordinance on Data Protection (DPO), as amended from time to time ("Swiss FADP").

e) "Data Protection Laws" means applicable laws governing the privacy and security of Personal Data, including, where applicable and without limitation, European Data Protection Laws, the CCPA, other U.S. state comprehensive privacy laws, Canadian Privacy Laws, and any other applicable privacy, artificial intelligence, data protection, or data security laws.

f) "Permitted Purpose" means processing of Personal Data (i) as necessary for the provision of the Services as set forth in greater detail in Schedule 1; (ii) as otherwise permitted by Data Protection Laws in connection with the Services; and (iii) to comply with legal obligations which do not conflict with Data Protection Laws.

g) "Personal Data" means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household in connection with the Services performed for Customer, including without limitation any information that qualifies as "personal information" or "personal data" under the Data Protection Laws applicable to Redesign.

h) "Restricted Transfer" means: (i) where the EU GDPR applies, a transfer of Personal Data from the European Economic Area to a country outside the European Economic Area that is not subject to an adequacy decision by the European Commission; (ii) where UK Data Protection Laws apply, a transfer of Personal Data from the United Kingdom to a country that is not subject to applicable UK adequacy regulations; and (iii) where the Swiss FADP applies, a transfer of Personal Data from Switzerland to a country that is not subject to an adequacy decision by the Swiss Federal Council.

i) "Security Breach" means a breach of security leading to unauthorized disclosure of or access to Personal Data in Redesign's possession, custody, or control.

j) "Sensitive Data" means (a) social security number, tax file number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) credit or debit card number (other than the truncated last four digits of a credit or debit card); (c) employment, financial, credit, genetic, biometric, or health information; (d) racial, ethnic, political, or religious affiliation, trade union membership, information about sexual life or sexual orientation, or criminal record; (e) account passwords; or (f) other information that falls within the definition of "special categories of data," "sensitive data," or "nonpublic personal information" under applicable Data Protection Laws or personal information as defined in applicable data breach notification laws.

k) “Services” means the services, products, applications, platforms, hosted or cloud-based services, technology, support, managed services, professional services, and other offerings provided or made available by Redesign under the Agreement, including Redesign Products and Redesign Applications.

l) "Standard Contractual Clauses" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to the EU GDPR ("EU SCCs"); and (ii) where the UK Data Protection Laws apply, the UK Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018 (the "UK Addendum").

II. Scope of DPA

a) This DPA applies to the extent that Redesign will process Personal Data on behalf of Customer in the provision of Services under the Agreement. For the avoidance of doubt, it is the intention of the Parties that Redesign be a "service provider," "processor," or "licensee" of Customer when required by applicable Data Protection Laws and that Customer be a "business," "controller," or "licensor" when required by applicable Data Protection Laws.

b) Redesign is not required to process Sensitive Data on behalf of Customer unless an applicable Order, SOW, or other written instrument executed by the Parties expressly identifies the categories and types of Sensitive Data and any additional safeguards required for such processing. Unless the Parties provide such written authorization, Customer will restrict Redesign’s access to Sensitive Data under Customer’s possession or control.

c) If Redesign inadvertently receives Sensitive Data not authorized under an applicable Order, SOW, or other written instrument executed by the Parties, Redesign will promptly notify Customer and, at Customer’s direction, securely delete or return such Sensitive Data. Redesign will not process such Sensitive Data except as necessary to identify, secure, return, or delete it or to comply with applicable Law. Redesign is not liable for unauthorized access to or use of Sensitive Data that Customer provided in violation of this Section, except to the extent directly caused by Redesign’s breach of its obligations under this DPA.

d) If any Data Protection Law imposes additional or overriding obligations to those set forth in this DPA with respect to processing of Personal Data or requires Customer and Redesign to enter into any additional agreements, including data export instruments, or to implement any additional security or organizational security measures to process Personal Data under the DPA, Customer shall ensure that it complies with the applicable Data Protection Law in advance of disclosing any Personal Data subject to such Data Protection Laws and the Parties agree to negotiate such additional obligations, agreements, or security measures in good faith. Any additional costs incurred by Redesign in implementing such additional obligations, agreements, or security measures shall be borne by Customer.

III. Customer's Obligations

a) The Parties agree that Customer is responsible for obtaining any consents required by applicable Data Protection Laws, as well as providing and ensuring the accuracy of any notices required to disclose Personal Data to Redesign or any Redesign subcontractor providing Services for use in accordance with the Agreement. Furthermore, Customer warrants and shall indemnify, defend, and hold harmless Redesign from any claims, damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees) arising from Customer's breach of its warranty that all Personal Data processed by Redesign in accordance with these terms has been obtained and provided to Redesign in accordance with all applicable laws and that there are lawful grounds for processing any and all Personal Data by Redesign or any Redesign subcontractor providing Services for use in accordance with the Agreement.

b) Customer is fully responsible for its compliance with the Data Protection Laws. If additional cooperation from Redesign is required to ensure such compliance, the Parties will negotiate in good faith to address the terms of such cooperation, including reimbursement of Redesign costs for such additional services or support with respect thereto.

IV. Redesign's Obligations

a) Redesign shall only process Personal Data for the Permitted Purpose and in accordance with Customer's instructions. The Agreement and this DPA constitute Customer's complete and final documented instructions to Redesign for the processing of Personal Data. Customer acknowledges that Redesign is reliant on Customer for instruction as to the extent to which Redesign is entitled to use and process Personal Data, and that Redesign is not liable for any claim, loss, damage, cost, or expense (including regulatory fines, penalties, and reasonable attorneys' fees) brought by a data subject, regulatory authority, or any third party to the extent that such claim arises from or relates to Customer's errors, misrepresentations, or instructions, and Customer shall indemnify, defend, and hold harmless Redesign from any such claims. Where Data Protection Laws require Redesign to process Personal Data under terms other than those of the Agreement, Redesign shall promptly notify Customer of such legal requirement before processing, unless the Data

Protection Laws prohibit such disclosure. Where required by Data Protection Laws, Redesign shall also notify Customer if Redesign determines any of Customer's instructions infringes applicable Data Protection Laws.

b) Schedule 1, Section B sets forth the subject matter, duration, nature, and purpose of processing and the categories of Personal Data and data subjects relevant to the Permitted Purpose. If the Parties authorize Redesign to process Sensitive Data under Section II(b), the applicable Order, SOW, or other written instrument executed by the Parties will identify the additional categories of Personal Data and data subjects, applicable processing activities, and any additional restrictions or safeguards required for the Sensitive Data.

V. Cooperation

a) Upon request, Redesign shall provide reasonable cooperation and any necessary assistance to Customer in (i) responding to any legally required inquiries, complaints, or other communication regarding its processing of Personal Data held by Redesign, (ii) any request from a data subject or consumer to exercise its rights under Data Protection Law (including access, correction, deletion, portability, as applicable) including by assisting with appropriate technical and organizational measures, and (iii) Customer's obligations under applicable Data Protection Laws including assisting with data protection impact assessments where applicable, in each case insofar as possible and taking into account the nature of Redesign's processing and the Personal Data available to Redesign. Unless instructed by Customer, Redesign will not itself respond to individual data subject or consumer requests; rather, Redesign will enable Customer to fulfil its obligations. Redesign shall respond to Customer's requests for assistance with data subject or consumer rights within ten (10) business days, or such shorter period as necessary to enable Customer to meet its legal obligations. Redesign shall be obliged to provide such assistance only insofar as the Customer cannot respond to such request on its own. Customer shall be responsible for all authentication and validation of any Personal Data given to Customer by Redesign as it relates to this Section.

b) Redesign shall provide reasonable cooperation at no additional charge for: (i) the first two (2) data subject access requests per calendar year; (ii) cooperation with supervisory authority inquiries; and (iii) initial breach response activities. Additional cooperation beyond these thresholds may be provided at Redesign's then-current hourly professional services rates.

c) Redesign shall promptly notify Customer of any request, complaint, claim, or other communication received by Redesign or a subcontractor from a third party regarding its processing of Personal Data.

VI. Restricted Transfers

a) If and to the extent that performance of any Services requires a Restricted Transfer, the Parties agree that the applicable terms attached as Schedule 3 to this DPA shall govern such Restricted Transfer.

b) For Restricted Transfers from the EEA, the Parties agree that the EU Standard Contractual Clauses (Commission Implementing Decision 2021/914, Module Two: Controller to Processor) are incorporated by reference and shall govern such transfers. The details in Schedule 1 shall serve as Annex I, and Schedule 2 shall serve as Annex II.

c) For Restricted Transfers from the UK, the UK Addendum to the EU SCCs (issued under s.119A(1) of the UK Data Protection Act 2018), as amended and as read together with the Data (Use and Access) Act 2025, shall apply.

d) For Restricted Transfers from Switzerland, the EU SCCs shall apply with the following modifications required by the Swiss Federal Data Protection and Information Commissioner ("FDPIC"): (i) references to the "GDPR" are read as references to the Swiss FADP; (ii) the FDPIC is the competent supervisory authority under Clause 13; (iii) the governing law under Clause 17 is Swiss law; (iv) the competent courts under Clause 18 are the courts of Switzerland; and (v) references to a "Member State" are not interpreted to exclude Swiss data subjects from exercising their rights in Switzerland.

e) When legally required, Redesign shall conduct and document a transfer impact assessment for Restricted Transfers under Redesign control and implement supplementary measures where necessary to ensure an essentially equivalent level of protection.

f) Redesign will not participate in (nor permit any sub-processor to participate in) any other Restricted Transfer unless made in compliance with European Data Protection Laws, provided that Redesign shall not be liable for any Restricted Transfers that occur due to circumstances beyond Redesign's reasonable control. Any other transfer of Personal Data by either Party outside of the country in which the Services are being provided and which is not a Restricted Transfer shall be in compliance with Data Protection Laws.

g) Alternative and Additional Mechanisms. Where Redesign is self-certified under the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, or the Swiss-U.S. Data Privacy Framework, transfers may alternatively rely on such framework for so long as it remains valid. If any transfer mechanism relied upon under this Section is invalidated, suspended, or held not to provide an adequate basis for a Restricted Transfer, the Parties will, without undue delay, cooperate in good faith to implement an alternative lawful transfer mechanism.

h) Global Service Delivery and Customer Restrictions. Redesign may provide the Services through Personnel, Affiliates, and Sub-processors located in the United States and other jurisdictions, including through follow-the-sun monitoring, support, maintenance, incident response, and engineering activities. Such Personnel may remotely access Customer systems and Personal Data as reasonably necessary to provide the Services, subject to this DPA, Redesign's security program, and applicable Data Protection Laws. Remote access does not change any primary hosting or storage location expressly stated in an Order or SOW.

Before entering into an Order or SOW, Customer shall identify in writing any governmental, regulatory, contractual, data-localization, citizenship, residency, security-clearance, or personnel-location restriction applicable to the Services or Customer data. Redesign is not contractually obligated to comply with any Customer-specific restriction that does not otherwise apply directly to Redesign under applicable law unless Redesign expressly accepts that restriction in the applicable Order, SOW, or written addendum. Redesign does not otherwise represent that Services will be performed exclusively from any country or by Personnel possessing any particular citizenship, residency, or security clearance.

Any location or personnel restriction identified after execution shall be addressed through a Change Order. Redesign may adjust the scope, fees, staffing model, service levels, or schedule to accommodate the restriction and may suspend affected Services if continued performance would violate applicable law or an agreed restriction. All cross-border processing remains subject to the transfer and Sub-processor provisions of this DPA.

VII. Security

a) Redesign shall implement and maintain an information security program that establishes reasonable and appropriate technical, organizational, and physical safeguards designed to protect Personal Data in its control or possession, taking into account the nature of Redesign's processing. A description of Redesign's information security program is attached as Schedule 2 to this DPA. To the extent required by applicable Data Protection Laws, upon request, Redesign shall make available to Customer information reasonably necessary to demonstrate compliance with this obligation.

b) The technical, organizational, and physical measures listed in Schedule 2 are subject to technological progress and advancement. As such, Redesign may implement alternative, adequate measures which meet or exceed the security level of the measures described in Schedule 2 and will notify Customer only if Redesign's implementation of alternative security measures results in a material diminution of the security of Redesign's overall information security program.

c) Upon Customer's written request, no more than once during any twelve-month period, Redesign will provide then-current customer-facing documentation describing Redesign's information security program and summaries of, or reports from, third-party security assessments, audits, or certifications that Redesign has obtained, if any. Redesign's disclosure obligations are subject to its confidentiality obligations and Customer's execution of Redesign's standard nondisclosure agreement if one is not already in effect. Redesign does not warrant that it holds or will maintain any specific third-party certification unless expressly stated in the Agreement.

d) Upon reasonable advance notice (not less than thirty (30) days), Customer or its designated third-party auditor may conduct an on-site or remote audit of Redesign's processing activities and security measures, not more than once per twelve (12) month period, unless a Security Breach has occurred. Unless a Security Breach has occurred or Customer has reasonable grounds to believe that Redesign is not in compliance with this DPA, Redesign may satisfy this requirement by providing its most recent SOC 2 Type II report or equivalent third-party audit report covering the relevant controls. Customer shall bear its own costs associated with any audit, and Redesign may charge reasonable fees for time spent by Redesign personnel in connection with any audit beyond the first eight (8) hours per calendar year.

e) Redesign shall notify Customer without undue delay, and in no event later than seventy-two (72) hours, after becoming aware of a verified Security Breach. Such notification shall include, to the extent known: (i) a description of the nature of the breach, including the categories and approximate number of data subjects and Personal Data records affected; (ii) the name and contact details of Redesign's data protection contact; (iii) the likely consequences of the breach; and (iv) the measures taken or proposed to address the breach, including measures to mitigate its possible adverse effects.

VIII. Sub-processors

a) The Parties agree that Redesign may subcontract its obligations to subcontractors as necessary to perform the Services under the Agreement. Redesign shall remain responsible for subcontractors' performance under the Agreement and shall enter into an agreement with subcontractors that impose commercially reasonable and substantially equivalent obligations as set forth in this DPA. Redesign also agrees that any Personnel or subcontractors who have access to Personal Data are bound to process Personal Data in accordance with Redesign's instructions and are subject to obligations to maintain confidentiality.

b) Redesign shall maintain a current list of sub-processors on its website or make such list available to Customer upon request.

c) Redesign shall provide Customer with at least thirty (30) days' prior written notice of any intended addition or replacement of sub-processors, including the sub-processor's name, location, and processing activities.

d) Customer may object to an intended addition or replacement of a subprocessor on reasonable grounds related to data protection within fifteen (15) days after receiving notice. The Parties will work in good faith to resolve the objection. If the Parties cannot resolve the objection within a reasonable period, Customer may terminate the affected Services upon written notice without an additional early-termination penalty. Such termination does not relieve Customer of accrued payment obligations or payment obligations for noncancelable third-party costs, reserved-capacity charges, minimum commitments, or other committed amounts identified in the applicable Order or SOW and incurred before the effective date of termination.

IX. Return and Destruction

Upon termination of the applicable Services, or during the term upon Customer's written request with respect to Personal Data no longer required for Redesign's performance of active Services, Redesign will, at Customer's direction, return or delete Personal Data hosted or stored in Redesign's active systems. Redesign is not required to return or delete Personal Data that applicable Law requires Redesign to retain. During the term, Redesign is not required to delete Personal Data reasonably necessary to perform active Services, maintain security, comply with the Agreement, or preserve applicable legal rights.

After Personal Data is deleted from Redesign's active systems, residual copies may remain in backups, logs, archives, disaster-recovery systems, and other systems where immediate deletion is technically infeasible. Such Personal Data will remain protected under this DPA and will not be actively processed except for security, restoration, legal compliance, or disaster-recovery purposes. Redesign will overwrite or securely delete residual copies according to its standard retention practices, not to exceed one (1) year, unless applicable Law requires longer retention.

Backup scope, frequency, retention, restoration, recovery-point objectives, and recovery-time objectives for Customer-specific Services apply only if expressly stated in the applicable Order or SOW.

X. Records of Processing Activities

Redesign shall maintain records of processing activities carried out on behalf of Customer as required by applicable Data Protection Laws, including: (a) the name and contact details of Redesign and Customer; (b) categories of processing carried out on behalf of Customer; (c) where applicable, transfers to third countries and documentation of suitable safeguards; and (d) a general description of technical and organizational security measures. Such records shall be made available to Customer or supervisory authorities upon request.

XI. Automated Decision-Making

a) Redesign shall not use Personal Data for automated decision-making, including profiling, that produces legal or similarly significant effects on data subjects, unless expressly authorized by Customer in writing.

b) If Customer authorizes such processing, Redesign shall implement appropriate safeguards, including the ability to provide meaningful information about the logic involved and enable human intervention upon request.

c) Redesign and its Affiliates will not use identifiable Personal Data processed on behalf of Customer to train or fine-tune any machine-learning or artificial-intelligence model unless Customer expressly authorizes such processing in an applicable Order, through a setting controlled by an Administrator designated by Customer, or through another documented instruction accepted by Redesign. Any such authorization constitutes Customer's documented processing instruction under this DPA. The Parties will document any resulting change in their respective roles under applicable Data Protection Laws. Redesign and its Affiliates may use aggregated, de-identified, or anonymized data that does not identify Customer or any data subject, and non-content usage data and telemetry, to develop, train, fine-tune, test, evaluate, validate, operate, and improve Redesign's models, systems, products, and services, where permitted by applicable Data Protection Laws.

XII. Liability; Data Security Cap

a) Except as set forth in this Section, each Party's liability under or in connection with this DPA is subject to the exclusions and limitations of liability set forth in the Agreement.

b) Data Security Cap. Notwithstanding any liability cap in the Agreement, in the event that Redesign's breach of its data privacy or data security obligations under the Agreement or this DPA is the direct and sole cause of a Security Breach, Redesign's aggregate

liability arising from such Security Breach shall not exceed one hundred thousand dollars ($100,000) in the aggregate (the "Data Security Cap"), which cap applies in place of, and supersedes, the general liability cap in the Agreement for such claims. In such event only, the following are deemed direct damages and are not excluded by the exclusion of damages in the Agreement: (i) the cost of providing legally required written notices to affected individuals; (ii) the cost of twelve (12) months of credit monitoring services for affected individuals who are also required to receive such written notice; and (iii) the cost of call center services for up to six (6) months for such individuals.

c) The Data Security Cap does not apply to the extent a higher amount is expressly agreed in a signed writing between the Parties. Nothing in this Section limits Customer's payment obligations or either Party's liability that cannot be limited under applicable law.

XIII. General Provisions

a) This DPA shall be governed by and construed in accordance with the governing law provisions of the Agreement, unless otherwise required by applicable Data Protection Laws.

b) In the event of any conflict between this DPA and the Agreement, this DPA shall prevail with respect to the processing of Personal Data.

c) This DPA shall remain in effect for so long as Redesign processes Personal Data on behalf of Customer.

Schedule 1: Data Processing Description

A. List of Parties

Data Exporter(s):

- Name: Customer or Customer Affiliate identified in the applicable Order or SOW
- Address: As set forth in the applicable Order or SOW or otherwise provided to Redesign
- Contact person's name, position, and contact details: As set forth in the applicable Order or SOW or otherwise provided to Redesign
- Activities relevant to the data transferred under these Clauses: See Section B
- Role: Controller

Data Importer(s):

- Name: The Drala Project, Inc. d/b/a The Redesign Group
- Address: 222 N Pacific Coast Hwy, Floor 10, El Segundo, CA, 90245
- Contact person's name, position, and contact details: As set forth in the applicable Order or SOW or otherwise provided to Customer
- Activities relevant to the data transferred under these Clauses: See Section B
- Role: Processor

B. Description of Processing

Subject Matter, Nature, and Purpose of Processing: Redesign processes Personal Data as reasonably necessary and proportionate to provide the Services on behalf of Customer under the Agreement. Processing may include collection, access, hosting, storage, organization, retrieval, consultation, use, analysis, indexing, transmission, integration, configuration, support, monitoring, security, troubleshooting, deletion, and other processing required for the Services.

Frequency of Processing and Transfers: Processing and transfers may occur continuously, periodically, intermittently, or upon Customer instruction throughout the term of the applicable Services.

Categories of Data Subjects: Customer’s and its Affiliates’ employees, contractors, consultants, temporary workers, representatives, administrators, Authorized Users, customers, prospective customers, suppliers, vendors, students, end users, and other individuals whose Personal Data is submitted to or processed through the Services.

Types of Personal Data: Names; physical and electronic contact information; business and professional information; user, account, and organizational identifiers; IP addresses; device and endpoint identifiers; authentication, access, permission, and authorization data; network, system, application, and security telemetry; logs and audit records; helpdesk, support, and ticket content; files and hosted-

application content; communications; prompts, inputs, and outputs submitted to or generated through AI-enabled functionality; and other non-Sensitive Data identified in the applicable Order or SOW.

Sensitive Data: No processing of Sensitive Data is intended unless expressly authorized under Section II(b). The applicable Order, SOW, or other written instrument authorizing Sensitive Data will identify the relevant categories, data subjects, processing activities, and additional safeguards.

Duration: Processing will continue during the term of the applicable Services and for the limited period following termination described in Section IX.

C. Competent Supervisory Authority

For transfers governed by the EU Standard Contractual Clauses, the competent supervisory authority will be determined under Clause 13 of the EU Standard Contractual Clauses based on the establishment or representative of the data exporter and the location of affected data subjects. For transfers governed by UK Data Protection Laws, the competent supervisory authority is the United Kingdom Information Commissioner's Office. For transfers governed by the Swiss FADP, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

Schedule 2: Security Program

Where applicable to the Services provided and for its own infrastructure, Redesign implements reasonable and appropriate technical, organizational, and physical safeguards designed to protect against unauthorized processing (such as unauthorized access, collection, use, copying, modification, disposal, or disclosure, unauthorized, unlawful, or accidental loss, destruction, acquisition, or damage) of Customer Personal Data in Redesign's custody or control.

1. Standards. Redesign aligns applicable portions of its operations with recognized industry security standards and frameworks, including the AICPA System and Organization Controls 2 (SOC 2) framework, the ISO/IEC 27001 Information Security Management Standard, and relevant NIST cybersecurity frameworks and publications, as applicable. These standards inform Redesign's Information Security Program but do not constitute a separate contractual certification or obligation unless expressly stated in the Agreement.

2. Security Policies. Redesign maintains a written Information Security Program that includes administrative, technical, and physical safeguards designed to protect Customer Personal Data. The program is reviewed at least annually and updated as necessary to address changes in risk, technology, and industry practices. Summary documentation of the Information Security Program will be made available to Customer upon request.

3. Data Governance and Minimization. Redesign maintains data governance practices designed to ensure that Customer Personal Data is classified, protected, and retained in accordance with applicable legal, regulatory, and contractual requirements. Redesign limits the collection, use, retention, and disclosure of Customer Personal Data to what is necessary to provide the Services and implements secure disposition procedures when such data is no longer required.

4. Training. Redesign requires all employees with access to Customer Personal Data to complete industry standard security and privacy training upon hire and periodically thereafter, including annual training, role-based training, and ongoing security awareness activities.

5. Zero Trust Architecture. Redesign incorporates Zero Trust security principles into its security architecture and access management practices, including: periodic verification of user and system identity using multi-factor authentication and behavioral monitoring; enforcement of least-privilege access and role-based permissions for systems and applications handling Customer Personal Data; network and application segmentation designed to reduce attack surface and limit lateral movement; and continuous monitoring of user, device, and system activity to detect anomalous or unauthorized behavior.

6. Access Controls. Redesign maintains access controls designed to limit physical and logical access to Customer Personal Data on a least-privileged and role-based basis, including: specific user credentials and multi-factor authentication for systems accessing Customer Personal Data; logging and monitoring of access to systems that store or process Customer Personal Data; regular review and timely removal of access for personnel who no longer require it; and enforcement of least-privilege, role-based access assignments and separation of duties where appropriate.

7. Secure Infrastructure. Redesign maintains a secure infrastructure environment that includes: logical separation of Customer environments and data where services utilize shared or multi-tenant infrastructure; firewalls, network segmentation, and secure network design; intrusion detection and prevention capabilities; encryption of Customer Personal Data in transit and at rest using

industry-standard encryption protocols (e.g., AES-256 or equivalent for data at rest and modern TLS protocols for data in transit); hardened system configurations and secure baselines; and malware protection, endpoint security controls, security event monitoring, alerting, and centralized log retention and protection.

8. Encryption and Key Management. Redesign uses industry-standard encryption protocols to protect Customer Personal Data in transit and at rest. Encryption keys are managed securely using access controls, segregation of duties, and rotation practices consistent with industry standards. Access to encryption keys is restricted to authorized personnel with a demonstrated business need.

9. Threat Monitoring and Vulnerability Management. Redesign employs threat monitoring and vulnerability management controls, including: continuous identification of vulnerabilities through automated scanning tools and industry threat intelligence; a vulnerability management process including risk-based prioritization and timely remediation; periodic penetration testing performed by qualified internal personnel or independent third-party providers; and Security Incident Response procedures for identification, investigation, and mitigation of suspected incidents involving Customer Personal Data.

10. Change Management and Secure Development. Redesign maintains change management processes designed to ensure that modifications to systems supporting the Services are reviewed, tested, and approved prior to deployment. Redesign follows secure development practices, including secure coding standards, code review, automated security scanning, and testing to detect and remediate security vulnerabilities throughout the development lifecycle.

11. Business Continuity, Disaster Recovery, and Backups. Redesign maintains business-continuity and disaster-recovery plans designed to support the availability and recoverability of Redesign systems used to provide the Services. Redesign periodically tests its business-continuity and disaster-recovery capabilities. These measures support Redesign's infrastructure and do not create any Customer-specific backup, archival, restoration, recovery-point, recovery-time, redundancy, or retention commitment. Any such Customer-specific commitment must be expressly stated in the applicable Order or SOW. Customer is responsible for selecting and purchasing any optional backup, retention, restoration, or disaster-recovery Services required for Customer's legal, regulatory, operational, or business requirements.

Schedule 3: Regulatory-Specific Addenda and Standard Contractual Clauses

This Schedule 3 supplements the DPA with additional terms required by specific Data Protection Laws. To the extent Redesign's Services involve processing of Personal Data governed by the laws referenced below, the applicable provisions shall apply. Capitalized terms not defined herein have the meanings set forth in the DPA or the applicable Data Protection Law.

1. U.S. State Privacy Laws

This Section applies to the extent Redesign processes personal information governed by the California Consumer Privacy Act ("CCPA"), the Colorado Privacy Act ("CPA"), the Connecticut Data Privacy Act ("CTDPA"), the Virginia Consumer Data Protection Act ("VCDPA"), or any other U.S. state comprehensive privacy law (collectively, "U.S. State Privacy Laws").

a) Roles and Relationship. Redesign acts as a "service provider," "processor," or equivalent designation under applicable U.S. State Privacy Laws. Customer acts as a "business," "controller," or equivalent designation.

b) Processing Limitations. Redesign shall: (i) process personal information only for the specific business purposes set forth in the Agreement and as instructed by Customer; (ii) not sell or share personal information, or use it for targeted advertising, cross-context behavioral advertising, or profiling in furtherance of decisions that produce legal or similarly significant effects, unless expressly authorized by Customer; (iii) not combine personal information received from Customer with personal information received from other sources, except as permitted by applicable law; (iv) provide at least the same level of privacy protection as required by applicable U.S. State Privacy Laws; (v) notify Customer if Redesign determines it can no longer meet its obligations under applicable U.S. State Privacy Laws; and (vi) permit Customer to take reasonable steps to stop and remediate any unauthorized use of personal information.

c) Consumer Rights Assistance. Redesign shall assist Customer in responding to verifiable consumer requests to exercise rights under applicable U.S. State Privacy Laws (including access, correction, deletion, portability, and opt-out rights) by implementing appropriate technical and organizational measures.

d) Data Protection Assessments and Cybersecurity. Redesign shall provide information reasonably necessary to enable Customer to conduct and document data protection assessments and risk assessments required by applicable U.S. State Privacy Laws, including the risk-assessment and cybersecurity-audit requirements of the California Privacy Protection Agency regulations, and shall reasonably cooperate with Customer's cybersecurity-audit obligations to the extent they relate to Redesign's processing.

e) Automated Decision-Making Technology (ADMT). Where Redesign deploys automated decision-making technology in processing personal information on Customer's behalf, Redesign shall, upon request, provide information reasonably necessary for Customer to meet its transparency, risk-assessment, and opt-out obligations under applicable U.S. State Privacy Laws and CPPA regulations.

f) Security. Redesign shall implement appropriate technical and organizational security measures as described in Schedule 2.

g) Sub-processors. Redesign shall engage sub-processors only pursuant to written contracts imposing materially equivalent obligations. For laws requiring notice and objection rights (including CPA, CTDPA, and VCDPA), Redesign shall provide Customer with at least thirty (30) days' prior written notice of any intended addition or replacement of sub-processors and an opportunity to object on reasonable data protection grounds.

h) Audits and Assessments. Redesign shall: (i) make available to Customer information necessary to demonstrate compliance with applicable U.S. State Privacy Laws; and (ii) allow for and contribute to reasonable assessments by Customer or Customer's designated assessor. Alternatively, Redesign may arrange for a qualified, independent assessor to conduct an annual audit using an appropriate control standard (such as SOC 2) and provide a report to Customer upon request.

i) Data Return and Deletion. At Customer's direction upon termination of Services, Redesign shall delete or return all personal information, unless retention is required by law.

j) Certification. Redesign certifies that it understands and will comply with the restrictions and obligations set forth in this Section.

2. Gramm-Leach-Bliley Act ("GLBA")

This Section applies to the extent Redesign processes Nonpublic Personal Information subject to GLBA (15 U.S.C. § 6801 et seq.) and the FTC Safeguards Rule (16 C.F.R. Part 314).

a) Safeguards. Redesign shall implement and maintain a written comprehensive information security program containing administrative, technical, and physical safeguards that comply with 16 C.F.R. § 314.4.

b) Notification Events. Consistent with the FTC Safeguards Rule breach-notification requirement (16 C.F.R. § 314.4(j)), Redesign shall notify Customer without undue delay of any notification event (as defined in the Safeguards Rule) affecting Nonpublic Personal Information processed on Customer's behalf, and shall provide information reasonably necessary to enable Customer to satisfy its own notification obligations.

c) Permitted Uses. Redesign may receive, hold, and process Nonpublic Personal Information solely to perform Services as directed by Customer and for Redesign's proper management and administration. Redesign shall not disclose such information except as required by law.

d) Customer Obligations. Customer shall not request Redesign to use or disclose Nonpublic Personal Information in any manner that would violate GLBA if done by Customer.

3. Controlled Unclassified Information ("CUI") and CMMC

This Section applies to the extent Redesign's Services involve CUI subject to Department of Defense standards or Cybersecurity Maturity Model Certification ("CMMC") requirements, as established under 32 C.F.R. Part 170 and implemented through DFARS 252.204-7021.

a) System Security Plan. Redesign shall maintain documentation describing system boundaries, interconnections, and security controls.

b) CMMC Controls. Redesign shall implement controls addressing: Access Control; Awareness and Training; Audit and Accountability; Configuration Management; Identification and Authentication; Incident Response; Maintenance; Media Protection; Personnel Security; Physical Protection; Risk Assessment; Security Assessment; System and Communications Protection; and System and Information Integrity, as applicable to the required CMMC level. The Parties acknowledge that CMMC requirements and their phased implementation are subject to change, and the applicable CMMC level and assessment obligations will be as set forth in the applicable SOW.

4. New York SHIELD Act

Redesign maintains a comprehensive information security program as described in Schedule 2, which is designed to comply with the data security requirements of the New York SHIELD Act (N.Y. Gen. Bus. Law § 899-bb).

5. European Data Protection Laws and International Transfers

This Section applies to the extent Redesign processes Personal Data subject to European Data Protection Laws (EU GDPR, UK Data Protection Laws, or Swiss FADP).

a) Processor Obligations. In accordance with GDPR Article 28 and, where applicable, Swiss FADP Article 9, Redesign shall: (i) process Personal Data only on documented instructions from Customer, unless required by applicable law (in which case Redesign shall notify Customer before processing, unless prohibited); (ii) ensure that persons authorized to process Personal Data are subject to confidentiality obligations; (iii) implement appropriate technical and organizational security measures pursuant to GDPR Article 32 and as described in Schedule 2; (iv) engage sub-processors only with Customer's prior general written authorization, and provide at least thirty (30) days' notice of any intended changes to sub-processors, giving Customer the opportunity to object; (v) assist Customer in responding to data subject requests and in fulfilling Customer's obligations under GDPR Articles 32-36, provided that, unless instructed by Customer, Redesign will not itself respond to individual data subject requests but will enable Customer to fulfil its obligations under Chapter III of the GDPR; (vi) at Customer's choice, delete or return all Personal Data upon termination of Services, unless retention is required by applicable law; (vii) make available information necessary to demonstrate compliance and allow for audits and inspections by Customer or Customer's designated auditor; and (viii) immediately inform Customer if an instruction infringes applicable data protection law.

b) Records of Processing. Redesign shall maintain records of processing activities as required by GDPR Article 30(2) and Swiss FADP Article 12 and make them available to Customer or supervisory authorities upon request.

c) Breach Notification. Redesign shall notify Customer without undue delay, and in no event later than seventy-two (72) hours, after becoming aware of a Personal Data Breach, providing information as required by GDPR Article 33(3). For Personal Data subject to the Swiss FADP, notification shall be made as soon as possible consistent with Swiss FADP requirements.

d) International Transfers. (i) For Restricted Transfers from the EEA, the EU SCCs (Commission Implementing Decision 2021/914, Module Two: Controller to Processor) are incorporated by reference; the details in Schedule 1 serve as Annex I and Schedule 2 as Annex II. (ii) For Restricted Transfers from the UK, the UK Addendum, as amended and read together with the Data (Use and Access) Act 2025, shall apply. (iii) For Restricted Transfers from Switzerland, the EU SCCs shall apply with the Swiss modifications set out in Section VI(d) of the DPA. (iv) The EU SCCs shall be governed by the law of Ireland and disputes resolved by the courts of Ireland; for UK transfers, the governing law shall be the laws of England and Wales. (v) The alternative and fallback mechanisms in Section VI(g) of the DPA apply.

e) Transfer Impact Assessment. Redesign shall conduct and document a transfer impact assessment for Restricted Transfers and implement supplementary measures where necessary to ensure an essentially equivalent level of protection.

f) Government Access Requests. If Redesign receives a legally binding request from a public authority for disclosure of Personal Data, Redesign shall (unless prohibited by law): (i) notify Customer promptly; (ii) challenge the request where there are reasonable grounds to consider it unlawful; and (iii) provide only the minimum information required.

6. Canadian Privacy Laws (PIPEDA and Quebec Law 25)

This Section applies to the extent Redesign processes Personal Information in connection with commercial activities subject to PIPEDA or substantially similar provincial legislation, including Quebec's Law 25.

a) Role. Redesign acts as a service provider processing Personal Information on behalf of Customer.

b) Compliance. Redesign shall comply with PIPEDA and applicable provincial privacy legislation, including Quebec's Law 25, including maintaining a privacy policy and ensuring Personnel are familiar with their obligations.

c) Collection, Use, and Disclosure. Redesign shall collect, use, and disclose Personal Information only as necessary for the Services or as authorized by Customer or required by law.

d) Security. Redesign shall protect Personal Information by making reasonable security arrangements against theft, loss, and unauthorized access, collection, use, disclosure, or disposal.

e) Access Requests. If Redesign receives a request for access to or correction of Personal Information, Redesign shall promptly refer the requestor to Customer and notify Customer of the request.

f) Personnel. Redesign shall ensure Personnel with access to Personal Information have agreed to confidentiality obligations and are familiar with Redesign's obligations under this Agreement and applicable law.

g) Sub-processors. Redesign shall require sub-processors to be bound by terms equivalent to this Section.

h) Cross-Border Transfers. Customer acknowledges that Personal Information may be processed outside Canada (including Quebec) using Redesign's cloud infrastructure, and Customer represents that it has provided all required notices and obtained all required consents, and conducted any privacy impact assessment required under Law 25, for such processing.

i) Breach Notification. Redesign shall notify Customer without undue delay after becoming aware of a verified Security Breach involving Personal Information.

j) Return or Destruction. Upon termination of the applicable Services, or during the term at Customer's written request with respect to Personal Information no longer required for active Services, Redesign shall return or destroy such Personal Information in accordance with Section IX.

k) Cooperation. Redesign shall cooperate with Customer in responding to inquiries from the Office of the Privacy Commissioner of Canada or the Commission d'accès à l'information du Québec and in any investigation regarding a breach of this Agreement or applicable privacy law.

7. Family Educational Rights and Privacy Act ("FERPA")

This Section applies to the extent Redesign processes education records or personally identifiable information derived from education records on behalf of Customer, as those terms are defined under FERPA, 20 U.S.C. § 1232g, and 34 C.F.R. Part 99.

a) School Official Designation. To the extent Redesign receives access to education records, Redesign is designated as a "school official" with "legitimate educational interests" as those terms are used in Customer's annual notification of FERPA rights, and Redesign's access is conditioned on that designation and on performance of an institutional service or function for which Customer would otherwise use its own employees.

b) Use Limitation. Redesign shall use education records solely to provide the Services as directed by Customer and shall not use or disclose education records for any other purpose, including marketing, advertising, profiling, or the training, fine-tuning, or improvement of artificial intelligence or machine-learning models, except with Customer's prior written consent.

c) Direct Control. Redesign shall be under the direct control of Customer with respect to the use and maintenance of education records.

d) Re-disclosure Prohibition. Redesign shall not re-disclose education records to any third party (including sub-processors) except as authorized by Customer, as required by law, or as otherwise permitted under 34 C.F.R. § 99.33, and shall require any authorized sub-processor to be bound by equivalent restrictions.

e) Security. Redesign shall implement reasonable and appropriate safeguards for education records consistent with Schedule 2.

f) Return and Deletion. Upon termination of the applicable Services, or during the term at Customer's written request with respect to education records no longer required for active Services, Redesign shall return or securely delete such education records in accordance with Section IX.

g) Customer Obligations. Customer is solely responsible for determining whether data disclosed to Redesign constitutes education records subject to FERPA, providing any directory-information opt-out notices, and ensuring Redesign's access is consistent with Customer's FERPA policies and annual notifications.

8. EU Artificial Intelligence Act

This Section applies to the extent Redesign provides, and Customer uses, an AI system or general-purpose AI model subject to the AI Act in connection with the Services. This Section does not apply to Products or Services that do not involve an AI system or model subject to the AI Act.

a) Roles. For each AI system made available under an Order, the Parties act in the roles assigned by the AI Act. Unless the applicable Order states otherwise: (i) where Redesign develops and makes available a proprietary Redesign AI system or model under its own name, Redesign acts as the "provider" and Customer acts as the "deployer"; (ii) where Redesign configures, integrates, resells, hosts, or operates a third-party AI system or model, the applicable third party is the provider and Redesign and/or Customer act as deployers, as applicable; and (iii) Customer becomes a provider, and assumes the corresponding obligations, if Customer puts its name or trademark on a high-risk AI system, substantially modifies such a system, or modifies its intended purpose such that it becomes high-risk, in each case as described in Article 25 of the AI Act.

b) Provider Obligations. To the extent Redesign acts as a provider, Redesign shall, as and to the extent required by the AI Act for the applicable risk classification, maintain technical documentation, implement risk-management and data-governance measures, provide

instructions for use and transparency information, maintain automatic logging capabilities, and reasonably cooperate with Customer in fulfilling Customer's deployer obligations.

c) Deployer Obligations. To the extent Customer acts as a deployer, Customer shall use the AI system in accordance with Redesign's instructions and Documentation, assign competent human oversight, ensure that input data is relevant and appropriate for the intended purpose and that Customer has the necessary rights to it, monitor the operation of the AI system, and inform Redesign without undue delay of any serious incident or malfunction of which Customer becomes aware.

d) Personal Data. Where an AI system processes Personal Data, this DPA governs such processing. Redesign shall not use Customer Personal Data to train, fine-tune, or improve AI systems or models except as permitted under Section XI of this DPA.

e) Allocation. Each Party is responsible for its own compliance with the AI Act in its assigned role and shall indemnify the other Party for Losses arising from the indemnifying Party's failure to comply with its role-specific obligations, subject to the limitations of liability in the Agreement.

9. Other Applicable Laws

To the extent Redesign's Services constitute processing of personal data governed by any Data Protection Law not specifically addressed in this Schedule 3, Redesign shall: (a) process personal data only as instructed by Customer; (b) implement appropriate security measures; (c) assist Customer in responding to data subject or consumer rights requests; (d) notify Customer of any data breach; (e) provide information necessary for Customer to conduct required assessments; and (f) ensure sub-processors are bound by equivalent obligations.

10. Hierarchy and Interpretation

In the event of a conflict between this Schedule 3 and the main body of the DPA, the provisions that provide greater protection for Personal Data shall prevail. If a specific regulatory addendum in this Schedule conflicts with a general provision, the specific addendum shall control with respect to Personal Data subject to that regulation.