redesign

Data Processing Agreement

This Data Processing Agreement ("DPA") is hereby incorporated into and governed by the Terms and Conditions located at 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) "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of natural persons with regard to the processing of personal data and on the free movement of such data, as amended or superseded from time to time ("EU GDPR"); the EU GDPR as it forms part of the law of the United Kingdom by virtue of section 3 of the UK European Union (Withdrawal) Act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 (together, "UK Data Protection Laws"); and the Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance ("Swiss DPA").

c) "Data Protection Laws" means applicable laws governing the privacy and security of Personal Data, including, where applicable, and without limitation, European Data Protection Laws, CCPA, and any other U.S. state comprehensive privacy laws.

d) "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.

e) "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.

f) "Restricted Transfer" means (i) where EU GDPR or the Swiss DPA applies, a transfer of Personal Data from the European Economic Area ("EEA") including Switzerland to a country outside of the EEA which is not the subject of an adequacy determination by the European Commission; and (ii) where UK GDPR applies, a transfer of Personal Data from the United Kingdom to any country which is not subject to adequacy regulations pursuant to Section 17A of the UK Data Protection Act.

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

h) "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.

i) "Standard Contractual Clauses" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementation 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) Notwithstanding the foregoing, the Parties acknowledge and agree that Redesign will not be required to process any Sensitive Data on behalf of Customer unless explicitly stated in a SOW, in which case the Customer will identify the categories and types of Sensitive Data which will be the subject of the processing in the applicable SOW. Unless the Parties agree that Redesign will process Sensitive Data on behalf of Customer in a SOW, Customer will restrict Redesign's access to any Sensitive Data under its possession or control.

c) If Redesign inadvertently receives Sensitive Data not authorized under a SOW, Redesign shall promptly notify Customer and, at Customer's direction, either securely delete such data or return it to Customer. Redesign shall not process such data except as necessary to comply with this paragraph. Redesign shall not be liable for any unauthorized access or use of Sensitive Data that is inadvertently received by Redesign.

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 ensured 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 hereto sets forth the subject matter, duration, nature and purpose of processing and the categories of Personal Data and data subject types relevant to the processing to fulfil the Permitted Purpose. If and to the extent that the Parties agree pursuant to Section II(b) hereof that Redesign will process Sensitive Data on behalf of Customer, the Parties will identify the additional categories of Personal Data and types of data subjects which will be the subject of the processing in the applicable SOW and any additional restrictions or security measures that need to be applied to the Sensitive Data, if any.

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. 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) shall apply.

d) For Restricted Transfers from Switzerland, the EU SCCs shall apply with the modifications required by the Swiss Federal Data Protection and Information Commissioner.

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.

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 on an annual basis, within thirty (30) days of said request, Redesign shall provide customer-facing documentation on the current state of Redesign's information security program and/or summaries or certificates of third-party certifications or security assessments, subject to Redesign's confidentiality obligations to third parties and provided that Customer executes Redesign's standard non-disclosure agreement if not already in place.

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.

IX. 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 such addition or replacement on reasonable grounds related to data protection within fifteen (15) days of receipt of notice. If Customer objects and the Parties cannot resolve the objection within a reasonable timeframe, Customer may terminate the affected Services without penalty upon written notice to Redesign.

X. RETURN AND DESTRUCTION

Notwithstanding any other provision of the Agreement to the contrary, upon termination of the Agreement or otherwise at Customer's written request, Redesign shall, at the direction of Customer, either return or delete Personal Data hosted or stored on its systems in the provision of Services unless required by law, rule, or regulation, or requested by any judicial, administrative, governmental, or regulatory authority to retain the Personal Data or if return or destruction would otherwise involve disproportionate efforts under the circumstances. After Personal Data has been deleted from Redesign's active systems, it may continue to exist in backups and logs for a period not to exceed one (1) year, after which such data shall be automatically overwritten or securely erased and/or destroyed in accordance with Redesign's data retention and destruction policies.

XI. 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.

XII. 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 shall not use Personal Data to train machine learning or artificial intelligence models for purposes unrelated to the Services without Customer's prior written consent. Notwithstanding the foregoing, Redesign may use aggregated, de-identified, or anonymized data that does not identify Customer or any data subject for analytics, service improvement, security monitoring, or product development purposes.

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

Element	Description
Subject Matter, Nature and Purpose of Processing	Processing as reasonably necessary and proportionate to perform the Services on behalf of Customer pursuant to the Agreement for business purposes and in accordance with the DPA. The foregoing includes project-based professional and managed Services (including, but not limited to, configuration, implementation, assessment, staff augmentation, unified communications, hosted and network services), maintaining or servicing accounts, providing storage, and other types of processing of Personal Data as necessary to provide the Services.
Categories of Data Subjects	Customers' employees and customers.
Types of Personal Data	Name, address (physical), email, phone number, IP address, system access/usage/authorization data, and other non-Sensitive Data. No processing of Sensitive Data or any special categories is intended; if and to the extent that processing of the foregoing is necessary under a specific Statement of Work, then the Parties will update the applicable SOW. Customer is solely responsible for determining and notifying Redesign of such processing and additional restrictions and/or security measures (if any) that are needed to be applied to the Sensitive Data transferred by Customer.
Duration	Continuous over the term of the Agreement plus the limited time following its termination in accordance with Section X.

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 American Institute of Certified Public Accountants (AICPA) System and Organization Controls 2 (SOC 2) framework, the ISO/IEC 27001 Information Security Management Standard, and relevant National Institute of Standards and Technology (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. These measures include:

- 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
- 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 in Redesign's custody or control on a least-privileged and role-based basis. Controls include:

- 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
- Enforcement of least-privilege, role-based access assignments, and separation of duties where appropriate

7. Secure Infrastructure

Redesign maintains a secure infrastructure environment designed to protect Customer Personal Data that includes:

- Logical separation of Customer environments and data where services utilize shared or multi-tenant infrastructure.
- Firewalls, network segmentation, and secure network design for internal and external communications
- 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, secure baselines, and procedures to remove unnecessary services, ports, and default accounts
- Malware protection and 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
- 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 (BCP) and Disaster Recovery (DR) plans designed to ensure the availability and recoverability of systems supporting the Services. These plans include data backup procedures, redundancy controls, and recovery processes intended to minimize disruption in the event of a system failure, disaster, or other business continuity incident. Redesign performs periodic testing of its BCP and DR capabilities to validate effectiveness and update procedures as necessary.

Redesign maintains backups of Customer Personal Data in accordance with its standard retention schedules and operational requirements. Extended backup retention, archival storage, or customer-specific backup requirements may be made available as an optional Service and may require additional fees. Customer is responsible for selecting any optional backup or retention Services needed to meet its legal, regulatory, 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 Provider'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 Provider processes personal information governed by the California Consumer Privacy Act ("CCPA"), Colorado Privacy Act ("CPA"), Connecticut Data Privacy Act ("CTDPA"), 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.** Provider 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.** Provider 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 Provider 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.** Provider 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.** Provider shall provide information reasonably necessary to enable Customer to conduct and document data protection assessments required by applicable U.S. State Privacy Laws.

e) **Security.** Provider shall implement appropriate technical and organizational security measures as described in Schedule 2.

f) **Sub-processors.** Provider 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), Provider 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.

g) **Audits and Assessments.** Provider 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, Provider 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.

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

i) **Certification.** Provider 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 Provider processes Nonpublic Personal Information subject to GLBA (15 U.S.C. § 6801 et seq.) and the FTC Safeguards Rule (16 C.F.R. § 314).

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

c) **Customer Obligations.** Customer shall not request Provider 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 Provider's Services involve CUI subject to Department of Defense standards or Cybersecurity Maturity Model Certification ("CMMC") requirements.

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

b) **CMMC Controls.** Provider 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.

4. New York SHIELD Act

Provider 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 Provider processes Personal Data subject to European Data Protection Laws (EU GDPR, UK Data Protection Laws, or Swiss DPA).

a) **Processor Obligations.** In accordance with GDPR Article 28, Provider shall:

i. Process Personal Data only on documented instructions from Customer, unless required by applicable law (in which case Provider 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 (security, breach notification, DPIAs, and prior consultation);

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.** Provider shall maintain records of processing activities as required by GDPR Article 30(2) and make them available to Customer or supervisory authorities upon request.

c) **Breach Notification.** Provider 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).

d) **International Transfers.**

i. 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.

ii. 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) shall apply.

iii. For Restricted Transfers from Switzerland, the EU SCCs shall apply with the modifications required by the Swiss Federal Data Protection and Information Commissioner.

iv. These Clauses shall be governed by the law of Ireland. Disputes shall be resolved by the courts of Ireland. For UK transfers, the governing law shall be the laws of England and Wales.

e) **Transfer Impact Assessment.** Provider 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 Provider receives a legally binding request from a public authority for disclosure of Personal Data, Provider 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)

This Section applies to the extent Provider processes Personal Information in connection with commercial activities subject to the Personal Information Protection and Electronic Documents Act ("PIPEDA") or substantially similar provincial legislation.

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

b) **Compliance.** Provider shall comply with PIPEDA and applicable provincial privacy legislation, including maintaining a privacy policy and ensuring Personnel are familiar with their obligations.

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

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

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

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

g) **Sub-processors.** Provider 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 using Provider's cloud infrastructure, and Customer represents that it has provided all required notices and obtained all required consents for such processing.

i) **Breach Notification.** Provider shall promptly notify Customer of any actual or suspected breach involving Personal Information.

j) **Return or Destruction.** Upon termination or Customer's written request, Provider shall return or destroy all Personal Information and Records, except as required by law.

k) **Cooperation.** Provider shall cooperate with Customer in responding to inquiries from the Privacy Commissioner and in any investigation regarding a breach of this Agreement or applicable privacy law.

7. Other Applicable Laws

To the extent Provider's Services constitute processing of personal data governed by any Data Protection Law not specifically addressed in this Schedule 3, Provider 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.

8. 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.