REPRISE DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") forms part of your Agreement with Reprise and contains certain terms relating to data protection, privacy, and security in accordance with Data Protection Legislation. In the event (and to the extent only) that there is a conflict between this DPA and the Agreement, this DPA shall control.

This DPA is between Customer and Reprise, Inc. and the most recent version date is April 20, 2023.

1. **DATA PROCESSING DEFINED TERMS.** In this DPA the following expressions shall, unless the context otherwise requires, have the following meanings:

1.1 The terms "controller", "data subject", "data protection impact assessment", "process", "processing", "processor", "supervisory authority" have the same meanings as in the Data Protection Legislation. Reprise and Customer hereby agree that Reprise is a "Service Provider" and Customer is the "Business", as defined under the CCPA and with respect to Personal Information.

1.2 "**Agreement**" means any agreement between Reprise Inc. and a customer for the Services. Such Agreement may have various titles, such as "Order," "Order Form," "Sales Order," "Subscription Agreement," or "Main Services and Subscription Agreement."

1.3 "**Customer**" or "**you**" means the customer that is identified on, and/or is a party to, the Agreement.

1.4 "**Data Privacy Framework**" or "**DPF**" means the EU-U.S. DPF, UK Extension to the EU-U.S. DPF, and Swiss-U.S. DPF developed by the U.S. Department of Commerce and the European Commission, UK Government, and Swiss Federal Administration to provide U.S. organizations with reliable mechanisms for personal data transfers to the United States from the European Union, United Kingdom, and Switzerland while ensuring data protection that is consistent with EU, UK, and Swiss law.

1.5 "**Data Protection Legislation**" means:

(a) the General Data Protection Regulation and the UK GDPR and all other applicable EU, EEA or European single market Member State laws or regulations or any update, amendment or replacement of same that apply to processing of Personal Data under the Agreement;

(b) all U.S. laws and regulations that apply to processing of Personal Data under the Agreement including, but not limited to, the California Consumer Privacy Act, as amended "CCPA," including as modified by the California Privacy Rights Act of 2020, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Personal Data Privacy and Online Monitoring Act, the Iowa Consumer Data Protection Act, the Nevada Privacy of Information Collected on the Internet from Consumers Act, the Maine Act to Protect the Privacy of Online Consumer Information, and the Utah Consumer Privacy Act, all upon their respective enforcement dates;

(c) all laws and regulations that apply to processing of Personal Data under the Agreement from time to time in place in Canada.

1.6 "**Personal Data**" means any information that relates to an identified or identifiable individual that is submitted to the Services by Customer, processed by Reprise for the purposes of delivering the Services to Customer. Appendix 2 to this DPA describes the Personal Data required to provide the Services.

1.7 "**Regulator**" means any supervisory authority or any replacement or successor body from time to time (or, to the extent required by the Customer, any other data protection or privacy regulator under Data Protection Legislation) or any federal or state agency in the United States (such as the FTC or a state Attorney General).

1.8 "**Reprise**" or "**us**" means Reprise Inc., a Delaware corporation located at 68 Harrison Ave #605, PMB 72297 , Boston, MA 02111, United States.

1.9 "**Security Incident**" means any confirmed breach of security that leads to the accidental, or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data processed by Reprise and/ or its Subprocessors in connection with the provision of the Services. For the avoidance of doubt, "Security Incident" does not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful login attempts, pings, port scans, denial of service attacks and other network attacks on firewalls or networked systems.

1.10 "**Services**" means the services ordered by Customer from Reprise under the Agreement.

1.11 "**Standard Contractual Clauses**" or "**SCC**" means the Standard Contractual Clauses annexed to the European Commission Implementing Decision of (EU) 2021/914 as of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to GDPR, and the UK SCCs effective August 27, 2021 as it pertains to transfers of Personal Data to third countries pursuant to the UK GDPR.

1.12 "**Subprocessor**" means any third-party processor engaged by Reprise to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA where such entity processes Personal Data.

2. **Relationship of the Parties.** In the provision of the Services to the Customer, Reprise is a processor of Personal Data for the purposes of Data Protection Legislation and a Service Provider for the purposes of CCPA. Customer processes such Personal Data as a controller.

3. **Term.** This DPA shall remain in force until such time as the Agreement is terminated (in accordance with its terms) or expires.

4. **Customer's Obligations.** Customer shall ensure and hereby warrants and represents that it is entitled to transfer the Personal Data to Reprise so that Reprise may lawfully process and transfer the Personal Data in accordance with this DPA. Customer shall ensure that any relevant data subjects have been informed of such use, processing, and transfer as required by the Data Protection Legislation and that lawful consents have been obtained (where appropriate). Customer shall ensure that any Personal Data processed or transferred to Reprise will be done lawfully and properly.

5. **Reprise's Obligations.**

5.1 Where Reprise is processing Personal Data for Customer as a processor, Reprise will:

(a) only do so on documented Customer instructions and in accordance with the Data Protection Legislation, including with regard to transfers of Personal Data to other jurisdictions or an international organization, and the parties agree that the Agreement constitutes such documented instructions of the Customer to Reprise to process Personal Data (including to locations outside of the relevant jurisdiction) along with other reasonable instructions provided by the Customer to Reprise (e.g. via email) where such instructions are consistent with the Agreement;

(b) ensure that all Reprise personnel involved in the processing of Personal Data are subject to confidentiality obligations in respect of the Personal Data;

(c) make available information necessary for Customer to demonstrate compliance with its applicable obligations under Data Protection Legislation where such information is held by Reprise and is not otherwise available to Customer through its account and user areas or on Reprise websites, provided that Customer provides Reprise with at least 14 days' written notice of such an information request;

(d) co-operate as reasonably requested by Customer to enable Customer to comply with any exercise of rights by a data subject afforded to data subjects by Data Protection Legislation in respect of Personal Data processed by Reprise in providing the Services;

(e) upon deletion by you, not retain Personal Data from within your account other than in order to comply with applicable laws and regulations and as may otherwise be kept in routine backup copies made for disaster recovery and business continuity purposes subject to our retention policies;

(f) cooperate with any Regulator in the performance of such Regulator's tasks where required;

(g) assist Customer as reasonably required where Customer:

(i) conducts a data protection impact assessment involving the Services (which may include by provision of documentation to allow Customer to conduct such assessment); or

(ii) is required to provide notice of a Security Incident to a Regulator or to a relevant data subject.

(h) will not (a) sell any Personal Information (as defined under the CCPA) for a commercial purpose, (b) collect, retain, use, disclose, or otherwise process Personal Information other than (1) to fulfill its obligations to Customer under the Agreement, (2) on the Customer's behalf, (3) for the Customer's operational purposes, (4) for Reprise's internal use as permitted by Data Protection Legislation, (5) to detect data security incidents or protect against fraudulent or illegal activity, or (6) as otherwise permitted under Data Protection Legislation, or (c) limit sharing of Personal Information when requested by a consumer or data subject; and

(i) will inform Customer if it comes to its attention that any instructions received by Customer infringe the provisions of Data Protection Legislation. Notwithstanding the foregoing, Reprise shall have no obligation to monitor or review the lawfulness of any instruction received from the Customer.

6. Subprocessors.

6.1 Customer agrees that Reprise may engage Subprocessors to process Personal Data on Customer's behalf. Reprise maintains a publicly available up-to-date list of all its Subprocessors accessible by Customer at any time. The Subprocessors currently engaged by Reprise and authorized by Customer are listed at https://www.reprise.com/subprocessors/. Reprise will: (i) enter into a written

agreement with each Subprocessor imposing data protection terms that require the Subprocessor to protect the Personal Data to the standard required by applicable Data Protection Legislation (and in substance, to the same standard provided by this DPA); and (ii) remain liable to Customer if such Subprocessor fails to fulfill its data protection obligations with regard to relevant processing activities under applicable Data Protection Legislation.

6.2 Reprise will (i) make available an up-to-date list of the Subprocessors it has appointed upon written request from Customer; and (ii) notify Customer if it adds any new Subprocessors at least fourteen (14) days prior to allowing such Subprocessor to process Personal Data. Customer must subscribe to receive notice of updates to the list of Subprocessors. Customer may object in writing to Reprise's appointment of a new Subprocessor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection under the Data Protection Laws. In such an event, the parties will discuss such concerns in good faith with a view to achieving resolution. If the parties are not able to achieve resolution, Customer, as its sole and exclusive remedy, may terminate the applicableAgreement or parts of the Service provided by the Subprocessor in question, effective on the date the Subprocessor starts providing services to Reprise.

7. Security.

7.1 Reprise has designed a commercially reasonable information security program that incorporates technical, administrative and organizational measures (in accordance with Appendix 1, attached hereto) that provide a level of security appropriate to the level of risk of possible unauthorized or unlawful processing, accidental loss of and/or damage to Personal Data. At least annually, Reprise conducts a risk assessment of the effectiveness of these technical, administrative and organizational measures for ensuring the security of the processing.

7.2 If Reprise becomes aware of any Security Incident, Reprise will take reasonable steps to notify Customer without undue delay and provide timely information (taking into account the nature of processing and the information available to Reprise) relating to the Security Incident as it becomes known or as is reasonable requested by Customer to allow Customer to fulfill its data breach reporting obligations under Data Protection Legislation. Reprise will take reasonable steps to contain, investigate and mitigate the effects of the Security Incident. Any notification of a Security Incident to the Customer does not constitute any acceptance of liability by Reprise.

8. Audits.

8.1 Customer acknowledges that Reprise is regularly audited by independent third-party auditors. Upon request, Reprise will supply a summary copy of its audit report to Customer so Customer can verify Reprise's compliance with the audit standard against which it has been assessed and this DPA. If Customer is subject to laws or regulations that require additional information, Reprise will, upon a written request by Customer, provide written responses to all reasonable requests for information made by Customer related to the processing of Personal Data.

8.2 Only to the extent Customer cannot reasonably satisfy its compliance requirements under Section 8.1 above, Customer will provide Reprise with at least one month's prior written notice of any audit, which may be conducted by Customer or an independent auditor appointed by Customer (provided that no person conducting the audit shall be, or shall act on behalf of, a competitor of Reprise) ("**Auditor**"). The scope of an audit will be as follows:

(a) Customer will only be entitled to conduct an audit once per subscription year unless otherwise legally compelled or required by a Regulator with established authority over the Customer to perform or facilitate the performance of more than 1 audit in that same year (in which circumstances Customer and Reprise will, in advance of any such audits, agree upon a reasonable reimbursement rate for Reprise's audit expenses).

(b) The scope of an audit will be limited to Reprise systems, processes, and documentation relevant to the processing and protection of Personal Data, and Auditors will conduct audits subject to any appropriate and reasonable confidentiality restrictions requested by Reprise.

(c) Customer will promptly notify and provide Reprise on a confidential basis with full details regarding any perceived non-compliance or security concerns discovered during the course of an audit.

8.3 The parties agree that, except as otherwise required by order or other binding decree of a Regulator with authority over the Customer, this Section 8 sets out the entire scope of the Customer's audit rights as against Reprise. The parties further agree that these rights fulfill Customer's right to take reasonable and appropriate steps to ensure that Reprise uses the Personal Data in a manner consistent with the Customer's obligations under the CCPA.

9. International Data Transfers.

9.1 To the extent applicable, for transfers of Personal Data from the European Economic Area to locations outside the European Economic Area (either directly or via onward transfer) that do not have adequate standards of data protection as determined by the European Commission, Reprise relies upon:

(a) the Standard Contractual Clauses;

(b) the UK SCC Addendum; provided that for purposes of Table 2 of UK SCC Addendum, Modules 2 and 3 of the EU SCCs shall apply and for purposes of Table 3 the details about the parties will be used to populate Annex 1.A of the UK SCC Addendum, the details in Appendix 2 will be used to complete the transfer details in Annex 1.B of the UK SCC Addendum, the list of Subprocessors pursuant to Section 6 hereof will be used to complete Annex III of the UK SCC Addendum and the representations contained in Section 7 hereof will be used to complete Annex II of the UK SCC Addendum;

(c) the Swiss Federal Act on Data Protection of 1992, provided that the Swiss Federal Data Protection and Information Commissioner shall be deemed the Regulator in Annex I.C under Clause 13 of the EU SCCs;

(d) the Data Privacy Framework; or

(e) such other appropriate safeguards, or derogations (to the limited extent appropriate), specified or permitted under the Data Protection Legislation.

9.2 To the extent any transfer of Personal Data is subject to the GDPR ("Data Transfer"), the parties will conduct such Data Transfer in accordance with this Section 9.2. Any Data Transfer will be conducted pursuant to the EU SCCs (which will be deemed executed by the parties as of the effective date of this DPA), and the following terms will apply:

(a) the clauses as set forth in Module Two (Controller to Processor) shall apply;

(b) the "data exporter" is the Customer;

(c) the "data importer" is Reprise;

(d) in Clause 7, the optional docking clause will apply;

(e) in Clause 9, Option 2 will apply, and the time period for prior notice of Subprocessor changes will be as set out in Section 6 of this DPA;

(f) in Clause 11, the optional language will not apply;

(g) in Clause 17, Option 1 will apply, and the Standard Contractual Clauses will be governed by Irish law;

(h) in Clause 18(b), disputes will be resolved before the courts of Ireland; and

(i) Annexes I and II of the SCCs are set forth in Appendix 1 and Appendix 2 below.

10. U.S. Data Transfers.

10.1 To the extent any transfer of Personal Data is subject to Data Protection Legislation in the United States, the parties agree to the following:

10.2 Reprise is prohibited from selling or sharing any Personal Data that Customer discloses to Reprise and Personal Data will be used only for the business purpose(s) set forth within the Agreement and will not be retained, used, or disclosed for any purpose other than the business purpose(s) specified in the Agreement or as otherwise permitted by the Data Protection Legislation;

10.3 Customer may request of Reprise to cooperate with it in responding to and complying with consumers' requests made pursuant to the Data Protection Legislation. If Reprise receives any consumer request made pursuant to the Data Protection Legislation with respect to Customer's account, Customer will provide the information necessary for Reprise to comply with the request. Both parties represent that, as appropriate between the parties, they can facilitate requests from consumers exercising their rights to know, delete, opt-out, non-discrimination, correct and limit use of Personal Data; and

10.4 Reprise will notify Customer after it makes a determination that it can no longer meet its obligations under applicable U.S. Data Protection Legislation.

11. General Provisions.

11.1 Liability for data processing. Each party's aggregate liability for any and all claims whether in contract, tort (including negligence), breach of statutory duty, or otherwise arising out of or in connection with this DPA shall be as set out in the Agreement, unless otherwise agreed in writing by the parties.

11.2 Conflict. In the case of conflict or ambiguity between: (i) the terms of this DPA and the terms of the Agreement, with respect to the subject matter of this DPA, the terms of this DPA shall prevail; (ii) the terms of any provision contained in this DPA and any provision

contained in the Standard Contractual Clauses, the provision in the Standard Contractual Clauses shall prevail.

11.3 Entire Agreement. The Agreement and this DPA represent the entire agreement between the parties and it supersedes any other prior or contemporaneous agreements or terms and conditions, written or oral, concerning its subject matter. Each of the parties confirms that it has not relied upon any representations or warranties provided outside of the Agreement inducing it to enter into the Agreement.

11.4 Severance. If any provision of this DPA is determined to be unenforceable by a court of competent jurisdiction, that provision will be severed and the remainder of terms will remain in full effect. Nothing in this DPA is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, nor authorize any party to make or enter into any commitments for or on behalf of any other party except as expressly provided herein.

11.5 Electronic Copy. This DPA is delivered as an electronic document.

11.6 Governing Law. This DPA shall be governed by the laws of Ireland and the parties submit to the exclusive jurisdiction of the Irish courts (in relation to all contractual and non-contractual disputes) except in the case of any alleged breach or breach of current or future privacy laws, regulations, standards, regulatory guidance, and self-regulatory guidelines at state or federal level in the United States of America, in which case the laws of the State of California shall govern unless otherwise dictated by that law.

IN WITNESS WHEREOF, the parties agree to be bound by the terms of this DPA as evidenced by their signatures below.

Customer:	Reprise, Inc.
Signature_____	Signature_____
Name: _____	Name: Evan Powell
Title:_____	Title: Co-Founder
Date: _____	Date:_____
Address: _____	Address: 68 Harrison Ave #605, PMB 72297
_____	Boston, MA 02111

APPENDIX 1

Description of the technical and organizational security measures implemented by Reprise

Reprise will maintain appropriate administrative, physical, and technical safeguards ("**Security Safeguards**") for protection of the security, confidentiality and integrity of Personal Data provided to it for provision of the Services to the Customer.

The Security Safeguards include the following:

1) **Domain: Organization of Information Security**.
   a) **Security Roles and Responsibilities.** Reprise personnel with access to Personal Data are subject to confidentiality obligations.
   b) **Risk Management Program.** Reprise performs a risk assessment where appropriate before processing Personal Data.
2) **Domain: Asset Management.**
   a) **Asset Handling.**
      i) Reprise has procedures for disposing of printed materials that contain Personal Data.
      ii) Reprise maintains an inventory of all hardware on which Personal Data is stored.
3) **Domain: Human Resources Security.**
   a) **Security Training.**
      i) Reprise informs its personnel about relevant security procedures and their respective roles. Reprise also informs its personnel of possible consequences of breaching the security rules and procedures.
4) **Domain: Physical and Environmental Security.**
   a) **Physical Access to Facilities.** Reprise limits access to facilities where information systems that process Personal Data are located to identified authorized individuals.
   b) **Protection from Disruptions.** Reprise uses a variety of industry-standard systems to protect against loss of data due to power supply failure or line interference.
   c) **Component Disposal.** Reprise uses industry-standard processes to delete Personal Data when it is no longer needed.
5) **Domain: Communications and Operations Management.**
   a) **Operational Policy.** Reprise maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Personal Data.
   b) **Data Recovery Procedures.**
      i) On a regular and ongoing basis, Reprise creates backup copies of Personal Data from which Personal Data may be recovered in the event of loss of the primary copy.
      ii) Reprise stores copies of Personal Data and data recovery procedures in a different

place from where the primary computer equipment processing the Personal Data is located.

iii) Reprise has specific procedures in place governing access to copies of Personal Data.

c) **Malicious Software.** Reprise has anti-malware controls to help avoid malicious software gaining unauthorized access to Personal Data, including malicious software originating from public networks.

d) **Data Beyond Boundaries**.

i) Reprise encrypts Personal Data that is transmitted over public networks.

e) **Event Logging**.

i) Reprise logs the use of its data-processing systems.

ii) Reprise logs access and use of information systems containing Personal Data, registering the access ID, timestamp, and certain relevant activity.

6) Domain: Information Security Incident Management.

a) Incident Response Process.

i) Reprise maintains an incident response plan.

ii) Reprise maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and remediation steps, if applicable.

7) Domain: Business Continuity Management.

a) Reprise's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Personal Data in its original state from before the time it was lost or destroyed.

8) **Access Control to Processing Areas**. Processes to prevent unauthorized persons from gaining access to the data processing equipment (namely telephones, database and application servers and related hardware) where the Personal Data are processed or used, to include:

a) establishing secure areas;

b) protection and restriction of access paths;

c) securing the mobile/cellular telephones;

d) data processing equipment and personal computers;

e) all access to the data centers where Personal Data are hosted is logged, monitored, and tracked;

f) the data centers where Personal Data are hosted is secured by a security alarm system, and other appropriate security measures; and

g) the facility is designed to withstand adverse weather and other reasonably predictable natural conditions, is secured by around-the-clock guards, keycard and/or biometric access (as appropriate to level of risk) screening and escort-controlled access, and is also supported by on-site backup generators in the event of a power failure.

9) **Access Control to Data Processing Systems.** Processes to prevent data processing systems

from being used by unauthorized persons, to include:

a) identification of the terminal and/or the terminal user to the data processor systems;
b) automatic time-out after 30 minutes or less of user terminal if left idle, identification and password required to reopen;
c) issuing and safeguarding of identification codes;
d) password complexity requirements (minimum length, expiry of passwords, etc.); and
e) protection against external access by means of an industrial standard firewall.

10) **Access Control to Use Specific Areas of Data Processing Systems.** Measures to ensure that persons entitled to use data processing systems are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that Personal Data cannot be read, copied, modified or removed without authorization, to include by:

a) implementing binding employee policies and providing training in respect of each employee's access rights to the Personal Data;
b) effective and measured disciplinary action against individuals who access Personal Data without authorization;
c) release of data to only authorized persons;
d) implementing principles of least privileged access to information which contains Personal Data strictly on the basis of "need to know" requirements;
e) production network and data access management governed by VPN, multi-factor authentication, and role-based access controls;
f) application and infrastructure systems log information to centrally managed log facility for troubleshooting, security reviews, and analysis; and
g) policies controlling the retention of backup copies which are in accordance with applicable laws and which are appropriate to the nature of the data in question and corresponding risk.

11) **Transmission Control.** Procedures to prevent Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media and to ensure that it is possible to check and establish to which bodies the transfer of Personal Data by means of data transmission facilities is envisaged, to include:

a) use of firewall and encryption technologies to protect the gateways and pipelines through which the data travels;
b) implementation of VPN connections to safeguard the connection to the internal corporate network;
c) constant monitoring of infrastructure (e.g. ICMP-Ping at network level, disk space examination at system level, successful delivery of specified test pages at application level); and
d) monitoring of the completeness and correctness of the transfer of data (end-to-end check).

12) **Storage Control.** When storing any Personal Data: it will be backed up as part of a designated backup and recovery processes in encrypted form, using a commercially supported encryption solution and all data defined as Personal Data stored on any portable or laptop computing device or any portable storage medium is likewise encrypted. Encryption solutions will be deployed with no less than a 128-bit key for symmetric encryption and a 1024 (or larger) bit key length for asymmetric encryption;
13) **Input Control.** Measures to ensure that it is possible to check and establish whether and by whom Personal Data has been input into data processing systems or removed, to include:
    a) authentication of the authorized personnel;
    b) protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
    c) utilization of user codes (passwords);
    d) proof established within data importer's organization of the input authorization; and
    e) ensuring that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are locked.
14) **Availability Control.** Measures to ensure that Personal Data are protected from accidental destruction or loss, to include infrastructure redundancy and regular backups performed on database servers.
15) **Segregation of Processing.** Procedures to ensure that data collected for different purposes can be processed separately, to include:
    a) separating data through application security for the appropriate users;
    b) storing data, at the database level, in different tables, separated by the module or function they support;
    c) designing interfaces, batch processes and reports for only specific purposes and functions, so data collected for specific purposes is processed separately; and
    d) barring live data from being used for testing purposes as only dummy data generated for testing purposes may be used for such.
16) **Vulnerability management program.** A program to ensure systems are regularly checked for vulnerabilities and any detected are immediately remedied, to include:
    a) all networks, including test and production environments, regularly scanned; and
    b) penetration tests are conducted regularly and vulnerabilities are remedied promptly.
17) **Data Destruction.** In the event of expiration or termination of the Agreement by either side or otherwise on request from the Customer following receipt of a request from a data subject or regulatory body:
    a) all Customer data shall be securely destroyed within 3 months; and
    b) all Customer data shall be purged from all Reprise and/or third-party storage devices including backups within 6 months of termination or receipt of a request from Customer unless Reprise is otherwise required by law to retain a category of data for longer periods. Reprise will ensure that all such data which is no longer required is destroyed to a level where it can be assured that it is no longer recoverable.

18) **Standards and Certifications.** Data storage solutions and/or locations have at least SOC 1 (SSAE 16) or SOC 2 reports – equivalent or similar certifications or security levels will be examined on a case-by-case basis.

APPENDIX 2

Purposes and Nature of Personal Data Processing, Categories of Personal Data, Data Subjects

The parties agree that the purpose and nature of the processing of Personal Data, the types of Personal Data and categories of data subjects are as set out in this Appendix 2.

Purposes and Nature of Processing	Reprise may process Personal Data as necessary to technically perform the Services, including where applicable: ● hosting and storage; ● backup and disaster recovery; ● technically improve the service; ● service change management; ● issue resolution; ● Providing secure, encrypted Services; ● applying new product or system versions, patches, updates and upgrades; ● monitoring and testing system use and performance; ● proactively detect and remove bugs; ● IT security purposes including incident management; ● maintenance and performance of technical support systems and IT infrastructure; ● migration, implementation, configuration and performance testing; ● making product recommendations; ● providing customer support; ● transferring data; and ● assisting with data subject requests (as necessary).

Categories of Personal data	The Customer may submit Personal Data to the Services, and may request for the Customer's respondents to submit Personal Data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, without limitation: ● Personal data of all types that may be submitted by the Customer's respondents to the Customer via users of the Services (such as via surveys or other feedback tools). For example: name, geographic location, age, contact details, IP address, profession, gender, financial status, personal preferences, personal shopping or consumer habits, and other preferences and other personal details that the Customer solicits or desires to collect from its respondents. ● Personal data of all types that may be included in forms hosted on the Services for the Customer (such as may be included in form questions). ● The Customer's respondents may submit special categories of Personal Data to the Customer via the Services, the extent of which is determined and controlled by the Customer.
Data Subjects	Data subjects include: ● Natural persons who submit Personal Data to Reprise via use of the Services (including via forms hosted by Reprise on behalf of the Customer); ● Natural persons whose Personal Data may be submitted to the Customer by respondents via use of the Services; ● Natural persons who are employees, representatives, or other business contacts of the Customer; or ● The Customer's users who are authorized by the Customer to access and use the Services.