Alida Subscriber Data Protection Schedule

Effective as of January 1, 2022

The Alida entity that has entered into a contract with the Subscriber ("**Alida**" or "**we**") serves the Subscriber and protects Subscriber Data in compliance with the terms of this Data Processing Schedule ("**Schedule**").

1. Definitions

A. "**Contract**" means the contract between Alida and Subscriber in which Alida agrees to make the Solution available to Subscriber, including all data sheets, service specifications, and other technical documentation, as amended from time to time, that may be incorporated by reference therein.

B. **"Backup"** means an extra copy of data to be used in the event that the original copy is damaged or unavailable. The extra copy of data is kept separately from the original copy.

C. **"Member"** means an individual whose data is processed in the Solution including when invited by or on behalf of Subscriber to visit, submit, view or comment on Subscriber Data on the Website and/or to participate in any forum, discussion, research, survey, study or any other means or form of data collection administered through the Solution.

D. **"Penetration Test"** means a search of software for misconfigurations and Security Defects by a security expert without access to the system's source code;

E. **"Personal Data"** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

F. **"Production System"** and **"Production Network"** means a computing environment that is used to host the Solution and is subject to access controls and management processes governing the introduction of changes;

G. **"Security Breach"** means any confirmed unauthorized access to, use of, or disclosure of Subscriber Data;

H. **"Security Defect"** means a technical deficiency in the software or hardware that, if exploited, could result in unauthorized access to the Solution or the Subscriber Data;

I. **"Security Questionnaire"** means any Subscriber developed or proprietary form or any other means that collects information on the security, privacy or data protection capabilities of Alida;

J. **"Security Scan"** means an automated search of a system for Security Defects without access to the system's source code;

K. "**Solution**" means the technology platform and automated services owned by Alida, including all standard upgrades and updates thereto but excluding any third-party products or software that may interoperate with Alida's technology platform;

L. **"Subscriber"** is a customer of Alida who has entered into a subscription agreement with Alida to access and use the Solution, and such term includes Subscriber's authorized users of the Solution;

M. **"Subscriber Data"** means information uploaded to or collected through the Solution by the Subscriber, or submitted to the Solution by Members;

N. **"Sub-Processor"** means a party that provides services to Alida for purposes of delivering the Solution and may have access to Subscriber Data; and

O. **"Supplier"** means a party that provides services to Alida for purposes of delivering the Solution and does not access Subscriber Data in provisioning such services.

P. **"Website"** means Subscriber's online operating instance of the Solution identified by and accessed via a domain owned by Subscriber.

2. Control and Ownership

Subscribers own and control all Subscriber Data. Alida does not use Subscriber Data, except: (a) in the interest and on behalf of the Subscriber; (b) as necessary to provide the Services; or (c) as contemplated or directed by the Contract. Alida reserves all rights to the Solution, Alida's technology and Alida's data, including any information that Alida discovers, creates or derives as it provides the Solution, except Subscriber Data.

3. Security

Alida applies technical, administrative and organizational data security measures that meet or exceed the requirements described in Alida's Statement of Technical and Organizational Measures (attached). Alida may update and modify its Statement of Technical and Organizational Measures from time to time, provided that Alida must not reduce the level of security provided thereunder, except with Subscriber's consent or with 90 days prior written notice.

4. Cooperation with Compliance Obligations

At Subscriber's reasonable request, Alida will (a) reasonably assist Subscriber with data access, deletion, portability and other requests, subject to compensation for any custom efforts required of Alida, and (b) enter into additional contractual agreements to meet specific requirements that are imposed by mandatory laws on Subscriber pertaining to Subscriber Data and that, due to their nature, can only be satisfied by Alida in its role as service provider or that Subscriber specifically explains and assigns to Alida in an addendum or amendment to the applicable Contract, subject to additional cost reimbursement or fees as appropriate. Where Subscriber is based within the EEA or the UK and is contracting with an Alida entity that is not based within the EEA or within an "adequate third country" (as determined by the European Commission) Alida will agree to the EU Commission Standard Contractual Clauses and UK International Data Transfer Addendum thereto for cross-border transfers. If Subscriber can no longer legally use Alida's products due to changes in law or technology, Alida shall allow Subscriber to terminate certain or all contracts and provide transition or migration assistance as reasonably required, subject to termination charges and fees as mutually agreed in good faith by the parties.

5. Security Breaches

In the event of a Security Breach, Alida shall use commercially reasonable efforts to: (i) contain and mitigate the impact of the Security Breach without undue delay; (ii) conduct an investigation into the cause of the Security Breach; (iii) notify Subscriber of the Security Breach without undue delay; and (iv) provide reasonably requested information to Subscriber to assist Subscriber in discharging its own legal obligations. For clarity, a respondent disclosing the contents of a Website to which they have been provided authorized access is not a Security Breach.

6. Audits

On an annual basis and at its own cost Alida will procure an independent audit of its security and privacy capabilities by a qualified professional of Alida's own choosing. Upon written request, Alida shall provide the resulting audit report ("**Audit Report**") to Subscriber. Upon Subscriber's written request, Alida will provide a commercially reasonable timeline for addressing any material defects in Alida's privacy and

security controls identified in the Audit Report ("**Identified Material Defects**"). Alida shall provide Subscriber or its designated auditor the opportunity to perform their own audit of Alida's privacy and security controls ("**Subscriber Audit**") only under the following circumstances: (i) the Audit Report is unavailable and Alida cannot provide a commercially reasonable timeline for when it will be made available to Subscriber; and (ii) the Audit Report includes Identified Material Defects for which Alida has not provided a remediation timeline. Any Subscriber Audit shall take place: (i) at Subscriber's sole expense; (ii) during Alida's normal business hours and over the course of no more than 2 business days: (iii) upon at least 10 business days' advance written notice to Alida with the notice including a clear scope statement and any evidence or other resources that Subscriber wishes to review; (iv) with Alida's written consent, which shall not be unreasonably withheld or delayed; (v) pursuant to appropriate confidentiality agreements; and (vi) only once per subscription year. For clarity, any request from Subscriber to complete a security questionnaire will be considered an invocation of audit rights, which Alida may satisfy with an Audit Report. Alida may also, at its own choosing, provide one of the following in lieu of responses to Subscriber's security questionnaire: (i) a completed Standard Information Gathering (SIG) questionnaire provided by Shared Assessments and The Santa Fe Group; (ii) a completed Cloud Security Alliance (CSA) questionnaire; or (iii) another reasonably equivalent standard questionnaire.

7. Hosting Locations

Alida's core systems, and associated data storage, are housed in a hosting facility at one of the following locations in accordance with the following: (i) Subscriber Data of Subscribers based in the Americas is hosted in Amazon Web Services' availability regions in the USA or Canada; (ii) Subscriber Data of Subscribers based in Europe, the Middle East or Africa is hosted in Amazon Web Services' availability region in Germany; and (iii) Subscriber Data of Subscribers based in the Asia-Pacific region is hosted in Amazon Web Services' availability region in Singapore. Alida may relocate its hosting facilities and all Subscriber Data therein provided that such relocation: (i) is posted to Alida's website at least 60 days in advance; and (ii) Alida keeps Subscriber Data within the same relative geographical region which is one of: (a) North America for Subscribers in the Americas; (b) the European Union for Subscribers in Europe, the Middle East or Africa; or (c) the Asia-Pacific region for Subscribers in Oceania, South East Asia, South Asia and East Asia. Alida shall maintain an up-to-date list of hosting facilities at https://www.alida.com/trust/legal/ or another page on its website with the same purpose ("**Subscriber Notices Page**"). For clarity, as between Alida and Subscriber, it is Subscriber's responsibility to comply with any regulations that require hosting of Subscriber Data within a specific jurisdiction. Alida maintains a global user store to manage Subscriber administrative user account authentication and routing to the relevant hosting region as described above. The data in this user store is housed in Canada.

8. Suppliers and Sub-Processors

Alida shall maintain appropriate legal agreements with all Suppliers and Sub-processors to ensure compliance with the obligations laid out within this Schedule and shall be responsible for its Suppliers' and Sub-processors' compliance with the terms of this Schedule. Alida shall maintain an up-to-date list of Suppliers and Sub-processors and their locations on its Subscriber Notices Page. Subscribers may register to receive automated notifications of updates to the list of Suppliers and Sub-processors.

9. Deletion and Anonymization

Upon termination of the Contract, Alida will permit Subscriber 30 days to export Subscriber Data from the Solution. Following such 30-day period, Alida will have no responsibility to retain any Subscriber Data and will thereafter permanently delete all Subscriber Data stored within the Solution. Subscriber Data Backups shall be securely deleted or overwritten 90 days thereafter. Upon request and if available, Alida will provide Subscriber with the ability to designate specific fields within a survey as Personal Data that should be overwritten after a Subscriber specified period of time has passed. Only fields associated with Members that have had their account set to an inactive status will be overwritten after the Subscriber's specified period of time has elapsed. For clarity, the Member's record will be considered anonymized by the Solution when the

fields specified by the Subscriber are overwritten such that they no longer contain identifying data; additionally the Solution will overwrite the Member's email address, user ID, name and telephone number. Once overwritten the original data is retained as a Backup for 90 days thereafter. Notwithstanding the preceding statements, Alida does not purge security and performance log data on Subscription termination, such data is eventually overwritten from our central logging system over time. Logs generally do not contain Member-provided data although they may contain email address and IP address, and other identifying information in some cases.

10. No Information Selling or Sharing for Cross‑Context Behavioral Advertising.

Alida does not accept or disclose any Subscriber Data as consideration for any payments, services or other items of value. Alida does not sell or share any Subscriber Data, as the terms "sell" and "share" are defined in the California Consumer Privacy Act of 2018, as amended, including by the California Privacy Rights Act ("**CCPA**"). Alida processes Subscriber Data only for the business purposes specified in the written Contract. Alida does not retain, use, or disclose Subscriber Data (a) for cross‑context behavioral advertising, or (b) outside the direct business relationship with the Subscriber. Alida does not combine Subscriber Data with other data if and to the extent this would be inconsistent with limitations on service providers under the CCPA.

11. EEA Personal Data

With respect to any Subscriber Data that is subject to the EU General Data Protection Regulation (GDPR) or similar laws of other countries as "personal data," Alida accepts the following obligations as a data importer, processor or subprocessor of Subscriber and warrants that Alida

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by European Union or EU Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; also, the processor shall immediately inform the controller if, in its opinion, an instruction infringes the GDPR, national data protection laws in the EU or other applicable law;
(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
(c) takes all measures required pursuant to Article 32 of the GDPR (security of processing);
(d) respects the conditions referred to in paragraphs 2 and 4 of Article 28 of the GDPR for engaging another processor;
(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, including, without limitation, right to access, rectification, erasure and portability of the data subject's personal data; (for the avoidance of doubt, processor shall only assist and enable controller to meet controller's obligations to satisfy data subjects' rights, but processor shall not respond directly to data subjects)
(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR (Security of personal data) taking into account the nature of processing and the information available to the processor;
(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

12. Notice of Changes

From time to time Alida may update its security and privacy practices. Any material changes will be posted on the Subscriber Notices Page at least 30 days prior to their coming into effect unless otherwise specified in the Contract. In the event Subscriber determines any such material change(s) are not acceptable to them, Subscriber may terminate its Contract with Alida as per its terms.

13. Integration

This Schedule is binding on Alida if and to the extent it is expressly agreed or incorporated by reference in a duly signed Contract. This Schedule shall not create third-party beneficiary rights. Alida does not accept or submit to additional requirements relating to Subscriber Data, except as specifically and expressly agreed in writing with explicit reference to the Contract and this Schedule.

Alida Statement of Technical and Organizational Measures

1. General

This Statement of Technical and Organizational Measures outlines the processes, infrastructure and policies that Alida has in place to protect its systems and Subscriber Data. Capitalized terms herein have the same meaning as in the Alida Subscriber Data Protection Schedule.

2. Policies and Governance

Alida has implemented the following governance structure with respect to its security and privacy policies and standards (the "**Policies**"):

A. Alida's Policies have been approved by Alida's executive (the "**Executive**");

B. A member of senior management is responsible for security and privacy at Alida and periodically reports to the Executive and Alida's board of directors (the "**Board**") on such matters;

C. Risks are centrally recorded and reported to the Executive and the Board as required;

D. Alida periodically reviews its Policies and supporting documentation for relevance;

E. Non-compliance with a Policy requires approvals in accordance with a clear authority framework;

F. Non-compliance without authorized approval of Policies has outcomes up to and including termination of employment;

G. Alida periodically reviews its Policies and supporting documentation for relevance;

H. On an annual basis, Alida conducts user security and privacy awareness education;

I. All employees sign-off on the Policies annually;

J. All new hires at Alida receive criminal background checks where permitted by law; and

K. All employees are subject to written confidentiality agreements.

3. Data Centre Security

Alida houses the Solution in enterprise class data centres that provide:

A. Independent annual audit reports of their security and availability capabilities. Such reports include but are not limited to: AICPA's Service Organization Controls ('SOC') audit reports or ISO27001 certifications;

B. Redundant cooling, fire suppression, power and communications; and

C. 24x7 guard services, physical access control and video surveillance.

4. Infrastructure Security

Alida has implemented the following security mechanisms:

A. The Solution is protected by firewalls or functionally equivalent technology that restricts traffic to only that which is required to provide the service;

B. Network traffic into the networking hosting the Solution is monitored by intrusion detection;

C. All access to the Solution and its supporting infrastructure is centrally logged;

D. 24/7 automated monitoring for malicious activity;

E. Bastion hosts and two factor authenticated VPN access into the Production Network; and

F. Anti-virus software.

5. Multi-tenant Environment

Alida provides a multi-tenant Solution which holds data for multiple Subscribers, and provides the following protections:

A. Each Website is dedicated to a single Subscriber;

B. Websites are uniquely identified by their domain name and underlying account identifier;

C. Access to Websites are only granted to the identities directly associated with the Subscriber's account;

D. Data is logically segregated using either separate database schemas or data attributes that are used by the application code to make access decisions; and

E. Detailed infrastructure logs are not available to any Subscriber.

6. Application Security

Alida provides the following controls within and around the Solution:

A. Username and password protected access to the administrator portal and optional integration with SAML 2.0 Identity Providers;

B. Authenticated access to the Website;

C. Logging of study creation/deletion/deployment as well as all user creation/modification/deletion; and

D. Secure development practices and use of safe software libraries. For the purposes of this section, a "safe software library" is one that is provided by the manufacturer that is free of known security defects and is designed such that developers are forced to use the library in a manner that does not unintentionally introduce security defects into the Solution.

7. Data Encryption

A. All connections to the Solution are protected using encrypted channels including but not limited to Transport Layer Security (TLS);

B. All Backups are encrypted; and

C. All systems storing Subscriber Data use disk storage that is encrypted at rest.

8. Operations

A. Alida has implemented processes including vulnerability management, incident response and security patching procedures to protect against known and emerging threats.

B. Changes to Production Systems can only be implemented by authorized system administrators following a defined quality assurance, change management, and approval process.

9. Disaster Recovery and Business Continuity

A. Alida shall maintain onsite snapshots and capacity sufficient to restore individual Websites within 48 hours with no more than 24 hours of data lost;

B. If Alida sends backups of the data offsite such backups will be encrypted and the keys for the encryption will remain under Alida's control; and

C. In the event of a catastrophic loss of an entire data centre, Alida shall use its commercially reasonable efforts to recover Subscriber's Website.

10. Privacy Policies and Logs

A. Alida maintains privacy policies to govern its own internal practices with regard to the secure and legal processing of Personal Data. Such policies address consent, collection limitation, data quality, limitation of use, disclosure, retention, transfers, data subject rights, and security as required by Applicable Privacy Regulation with regard to the processing of Personal Data. "**Applicable Privacy Regulation**" includes, but is not limited to:

i. *The Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") of Canada;

ii. The General Data Protection Regulation 2016/679 ("**GDPR**");

iii. The Federal Privacy Act 1988 of Australia;

iv. The Personal Data Protection Act 2012 of Singapore; and

v. The California Consumer Privacy Act ("**CCPA**").

B. Alida will retain logs containing personal information such as email addresses and IP addresses as well as actions taken on the Solution for security and monitoring purposes.

11. Security Testing

A. Alida will conduct an annual Penetration Test of the Solution using an external provider determined in Alida's sole discretion. Once identified Security Defects are remediated, Alida will confirm such remediation, or will arrange for same external provider to provide confirmation thereof;

B. Alida will conduct monthly Security Scans of the Solution;

C. Upon request by Subscriber, Alida will provide evidence that such Penetration Testing and Security Scanning has been performed;

D. Once per subscription year and with at least ten (10) business days of notice, Subscriber or its agent, may perform its own Penetration Testing against a Website provided by Alida, not the Subscriber's Website. Subscriber agrees to forego this right if Alida, in its sole discretion, offers an equivalently scoped report that is no more than twelve (12) months old;

E. Notwithstanding the preceding limitations of Penetration Testing frequency, additional testing to confirm that issues previously reported have been remediated are not limited in frequency;

F. At times mutually agreed between the parties, a Subscriber or its agent, may perform Security Scanning against its own Website once their methodology has been reviewed and approved by Alida;

G. Such annual Penetration Testing or Security Scanning by the Subscriber is in addition to the audit rights as provided in the Alida Subscriber Data Protection Schedule;

H. Alida may reasonably withhold approval for Penetration Testing or Security Scanning if there is reason to believe that the methodology the Subscriber or its agent will use disrupts the performance, availability or integrity of the Solution;

I. If Penetration Testing or Security Scanning by Subscriber or its agent disrupts the performance, availability or integrity of the Solution then Alida may direct Subscriber to immediately stop or cause

to be stopped all Penetration Testing of Security Scanning activity until such time Alida is satisfied as to the reason for disruption being addressed;

J. Subscriber will provide all information reasonably requested by Alida on the nature of their Penetration Testing and Security Scanning activities prior to commencing their work. Such information includes but is not limited to: source IP addresses, contact information, employee or agent names and times of testing;

K. Subscriber or its agent will comply with Alida's guidance on performing Penetration Testing and Security Scanning and in return Alida will furnish Subscriber with the necessary access to perform such Penetration Testing and Security Scanning;

L. If Subscriber requires that identified Security Defects be remediated, Subscriber or its agent must provide in writing the full details of the Security Defect such that Alida may independently assess, replicate and verify the existence of the Security Defect; and

M. Within ten (10) business days of Alida confirming the existence of the reported Security Defects Alida will provide, upon request, a remediation plan in accordance with the timelines in the following section.

12. Security Defect Remediation

A. Alida uses industry standard scoring techniques, such as Common Weakness Scoring System (CWSS) and Common Vulnerability Scoring System (CVSS), for evaluating the severity of any identified security defect. Alida may, at its own discretion, replace them with equivalent scoring techniques.

B. Alida will score a security defect using the aforementioned techniques and categorize defects by impact as follows:

Common impact name	CVSS	CWSS
Critical	9.0 to 10.0	90 to 100
High	7.0 to 8.9	70 to 89
Medium	4.0 to 6.9	40 to 69
Low	0.0 to 3.9	0 to 39

C. Alida will remediate Security Defects in our Solution using the following schedule once the reported Security Defect is confirmed:

Common impact name	Timing
Critical	Promptly and not more than fourteen (14) days
High	Within forty-five (45) days
Medium	Within ninety (90) days
Low	Within one hundred and eighty (180) days

D. Alida, at its own discretion, may implement a temporary solution to the Security Defect to achieve the timelines listed above. Such temporary solutions may include temporarily disabling or altering specific functionality, while working to implement a permanent solution to the Security Defect. Should Alida choose to temporarily disable or alter functionality to address a Security Defect, Subscriber will not treat such actions as a reduction in service;

E. Alida may reasonably defer remediation of a reported security defect for reasons including, but not limited to:

    a. The Security Defect is reported too late in the current release cycle to safely include relative to our change management practices;

    b. A planned change or fix will address the Security Defect in a reasonable time frame; or

    c. All available resources are already working on a Security Defect of a greater impact.

F. Alida may reasonably decline to remediate a Security Defect if the security defect provides no reasonable path for gaining access to Subscriber Data or the Solution.