Datenschutzvereinbaung für Alida-Kunden

Gültig ab dem 1. Januar 2022

Die Alida-Gesellschaft, die einen Vertrag mit dem Kunden abgeschlossen hat ("**Alida**" oder "**wir**"), dient dem Kunden und schützt die Daten des Kunden in Übereinstimmung mit den Bedingungen dieses Datenverarbeitungsplans ("**Plan**").

1. Begriffsbestimmungen

A. "**Vertrag**" bezeichnet den Vertrag zwischen Alida und dem Kunden, in dem sich Alida verpflichtet, dem Kunden die Plattform zur Verfügung zu stellen, einschließlich aller Datenblätter, Leistungsbeschreibungen und sonstiger technischer Unterlagen in ihrer jeweils gültigen Fassung, auf die darin Bezug genommen werden kann.

B. "**Backup**" bezeichnet eine zusätzliche Kopie von Daten für den Fall, dass die Originalkopie beschädigt wird oder nicht mehr verfügbar ist. Die zusätzliche Kopie der Daten wird getrennt von der Originalkopie aufbewahrt.

C. "**Mitglied**" bezeichnet eine Person, deren Daten auf der Plattform verarbeitet werden, auch wenn sie von oder im Namen des Kunden eingeladen wird, die Kundendaten auf der Website zu besuchen, einzureichen, zu betrachten oder zu kommentieren und/oder an einem Forum, einer Diskussion, einer Forschung, einer Umfrage, einer Studie oder einem anderen Mittel oder einer Form der Datenerfassung teilzunehmen, die über die Plattform verwaltet werden.

D. "**Penetrationstest**" bezeichnet die Untersuchung von Software auf Fehlkonfigurationen und Sicherheitsmängel durch einen Sicherheitsexperten ohne Zugriff auf den Quellcode des Systems;

E. "**Personenbezogene Daten**" sind alle Informationen über eine bestimmte oder bestimmbare natürliche Person ("betroffene Person"); als bestimmbar wird eine natürliche Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

F. "**Produktionssystem**" und "**Produktionsnetzwerk**" bezeichnet eine Computerumgebung, die zum Hosten der Plattform verwendet wird und Zugangskontrollen und Verwaltungsprozessen unterliegt, die die Einführung von Änderungen regeln;

G. "**Sicherheitsverletzung**" bezeichnet jeden bestätigten unbefugten Zugriff auf, die Nutzung von oder die Offenlegung von Teilnehmerdaten.

H. "**Sicherheitsmangel**" bezeichnet einen technischen Mangel in der Software oder Hardware, der, wenn er ausgenutzt wird, zu einem unbefugten Zugriff auf die Plattform oder die Kundendaten führen könnte;

I. "**Sicherheitsfragebogen**" ist ein vom Kunden entwickeltes oder eignes Formular oder ein anderes Mittel, mit dem Informationen über die Sicherheit, den Schutz der Privatsphäre oder die Datenschutzfunktionen von Alida gesammelt werden;

J. "**Sicherheitsscan**" bezeichnet eine automatisierte Suche eines Systems nach Sicherheitsmängeln ohne Zugriff auf den Quellcode des Systems;

K. "**Plattform**" bezeichnet die Technologieplattform und die automatisierten Dienste, die Eigentum von Alida sind, einschließlich aller Standard-Upgrades und -Updates, jedoch ohne Produkte oder Software von Drittanbietern, die mit der Technologieplattform von Alida zusammenarbeiten können;

L. "**Kunde**" ist ein Kunde von Alida, der einen Abonnementvertrag mit Alida abgeschlossen hat, um auf die Plattform zuzugreifen und sie zu nutzen, und dieser Begriff schließt die autorisierten Benutzer des Kunden der Plattform ein;

M. "**Kundendaten** sind Informationen, die vom Kunden in die Plattform hochgeladen oder über die Plattform gesammelt oder von Mitgliedern an die Plattform übermittelt werden;

N. "**Unterauftragsverarbeiter**" bezeichnet eine Partei, die Alida zum Zweck der Bereitstellung der Plattform-Dienstleistungen erbringt und Zugang zu den Daten des Teilnehmers haben kann;

O. "**Dienstleister**" bezeichnet eine Partei, die Alida Dienstleistungen zum Zweck der Bereitstellung der Plattform anbietet und bei der Bereitstellung dieser Dienstleistungen nicht auf die Daten des Teilnehmers zugreift.

P. "**Website**" bezeichnet die Online-Instanz der Plattform, die durch eine im Besitz des Kunden befindliche Domain identifiziert wird und auf die über diese Domain zugegriffen wird.

2. Kontrolle und Eigentum

Der Kunde ist Eigentümer aller Kundendaten und kontrolliert diese. Alida verwendet die Daten des Kunden nicht, außer: (a) im Interesse und im Auftrag des Kunden; (b) soweit dies für die Erbringung der Dienstleistungen erforderlich ist; oder (c) wie im Vertrag vorgesehen oder angewiesen. Alida behält sich alle Rechte an der Plattform, der Technologie von Alida und den Daten von Alida vor, einschließlich aller Informationen, die Alida bei der Bereitstellung der Plattform identifiziert, erstellt oder ableitet, mit Ausnahme der Daten des Kunden.

3. Sicherheit

Alida wendet technische, administrative und organisatorische Datensicherheitsmaßnahmen an, die den in der Beschreibung der technischen und organisatorischen Maßnahmen von Alida (im Anhang) definierten Anforderungen entsprechen oder diese übertreffen. Alida ist berechtigt, die Beschreibung der technischen und organisatorischen Maßnahmen von Zeit zu Zeit zu aktualisieren und zu ändern, wobei Alida das Sicherheitsniveau nicht verringern darf, es sei denn, der Kunde stimmt zu oder wird 90 Tage vorher schriftlich informiert.

4. Mitwirkung bei der Erfüllung von Compliance-Verpflichtungen

Auf angemessenen Antrag des Kunden wird Alida (a) den Kunden in angemessener Weise bei Datenzugriff, -löschung, -übertragbarkeit und anderen Anfragen unterstützen, vorbehaltlich einer Entschädigung für die von Alida geforderten individuellen Bemühungen, und (b) zusätzliche vertragliche Vereinbarungen treffen, um spezifische Anforderungen zu erfüllen, die dem Kunden durch zwingende Gesetze in Bezug auf die Daten des Kunden auferlegt werden und die aufgrund ihrer Natur nur von Alida in ihrer Rolle als Dienstleister erfüllt werden können oder die der Kunde ausdrücklich erklärt und an Alida in einem Nachtrag oder einer Änderung des anwendbaren Vertrages richtet, vorbehaltlich zusätzlicher Kostenerstattung oder Gebühren. Wenn der Kunde im EWR oder im Vereinigten Königreich ansässig ist und einen Vertrag mit einer Alida-Gesellschaft abschließt, die nicht im EWR oder in einem "angemessenen Drittland" (wie von der Europäischen Kommission festgelegt) ansässig ist, wird Alida den Standardvertragsklauseln der EU-Kommission und dem Zusatz zum internationalen Datentransfer im Vereinigten Königreich für grenzüberschreitende Übertragungen zustimmen. Wenn der Kunde die Produkte von Alida aufgrund von Gesetzes- oder Technologieänderungen nicht mehr rechtmäßig nutzen kann, gestattet Alida dem Kunden, bestimmte oder alle Verträge zu kündigen, und bietet ihm bei Bedarf Unterstützung bei der Umstellung oder Migration, vorbehaltlich der zwischen den Parteien nach Treu und Glauben vereinbarten Kündigungskosten und -gebühren.

5. Sicherheitsverletzungen

Im Falle eines Sicherheitsverstoßes unternimmt Alida wirtschaftlich vertretbare Anstrengungen, um: (i) die Auswirkungen des Sicherheitsverstoßes unverzüglich einzudämmen und abzumildern; (ii) eine Untersuchung der Ursache des Sicherheitsverstoßes durchzuführen; (iii) den Kunden unverzüglich über den Sicherheitsverstoß zu informieren; und (iv) dem Kunden angemessen angeforderte Informationen zur Verfügung zu stellen, um den Kunden bei der Erfüllung seiner eigenen rechtlichen Verpflichtungen zu unterstützen. Zur Klarstellung: Wenn ein Befragter den Inhalt einer Website offenlegt, zu der er autorisierten Zugang erhalten hat, stellt dies keinen Sicherheitsverstoß dar.

6. Überprüfungen

Alida wird jährlich auf eigene Kosten ein unabhängiges Audit ihrer Sicherheits- und Datenschutzkapazitäten durch einen qualifizierten Experten nach Wahl von Alida durchführen lassen. Auf schriftliche Anfrage wird Alida den daraus resultierenden Prüfbericht ("**Prüfbericht**") dem Kunden zur Verfügung stellen. Auf schriftliche Anfrage des Kunden wird Alida einen wirtschaftlich vertretbaren Zeitplan für die Behebung der im Audit-Bericht festgestellten wesentlichen Mängel bei den Datenschutz- und Sicherheitskontrollen von Alida ("**festgestellte wesentliche Mängel**") vorlegen. Alida wird dem Kunden oder dem von ihm beauftragten Prüfer die Möglichkeit geben, eine eigene Prüfung der Datenschutz- und Sicherheitskontrollen von Alida durchzuführen (" **Kunden-Audit**"), und zwar nur unter den folgenden Umständen: (i) der Audit-Bericht ist nicht verfügbar und Alida kann keinen wirtschaftlich vertretbaren Zeitpunkt nennen, wann er dem Kunden zur Verfügung gestellt wird; und (ii) der Audit-Bericht enthält identifizierte wesentliche Mängel, für die Alida keinen Zeitplan zur Behebung vorgelegt hat. Ein Audit des Kunden findet statt: (i) auf eigene Kosten des Kunden; (ii) während der normalen Geschäftszeiten von Alida und über einen Zeitraum von nicht mehr als zwei Geschäftstagen; (iii) nach schriftlicher Ankündigung an Alida mit einer Frist von mindestens zehn Geschäftstagen, wobei die Ankündigung eine eindeutige Erklärung zum Umfang und alle Beweise oder anderen Ressourcen enthält, die der Kunde zu überprüfen wünscht; (iv) mit der schriftlichen Zustimmung von Alida, die nicht unangemessen verweigert oder verzögert werden darf; (v) gemäß entsprechender Vertraulichkeitsvereinbarungen; und (vi) nur einmal pro Vertragsjahr. Der Klarheit halber wird jede Aufforderung des Kunden, einen Sicherheitsfragebogen auszufüllen, als Inanspruchnahme von Prüfungsrechten betrachtet, denen Alida mit einem Prüfungsbericht nachkommen kann. Alida kann nach eigenem Ermessen anstelle der Antworten auf den Sicherheitsfragebogen des Kunden auch einen der folgenden Fragebögen zur Verfügung stellen: (i) einen ausgefüllten Standard Information Gathering (SIG)-Fragebogen, der von Shared Assessments und The Santa Fe Group zur Verfügung gestellt wird; (ii) einen ausgefüllten Cloud Security Alliance (CSA)-Fragebogen; oder (iii) einen anderen, angemessen gleichwertigen Standardfragebogen.

7. Hosting-Standorte

Die Kernsysteme von Alida und die zugehörige Datenspeicherung sind in einer Hosting-Einrichtung an einem der folgenden Standorte untergebracht: (i) Kundendaten von Kunden mit Sitz in Amerika werden in den Verfügbarkeitsregionen von Amazon Web Services in den USA oder Kanada gehostet; (ii) Kundendaten von Kunden mit Sitz in Europa, dem Nahen Osten oder Afrika werden in der Verfügbarkeitsregion von Amazon Web Services in Deutschland gehostet; und (iii) Kundendaten von Kunden mit Sitz im asiatisch-pazifischen Raum werden in der Verfügbarkeitsregion von Amazon Web Services in Singapur gehostet. Alida kann seine Hosting-Einrichtungen und alle darin befindlichen Kundendaten verlagern, vorausgesetzt, dass eine solche Verlagerung: (i) mindestens 60 Tage im Voraus auf der Website von Alida bekannt gegeben wird; und (ii) Alida die Kundendaten innerhalb derselben relativen geografischen Region aufbewahrt, die eine der folgenden ist: (a) Nordamerika für Kunden in Nord- und Südamerika; (b) die Europäische Union für Kunden in Europa, dem Nahen Osten oder Afrika; oder (c) die asiatisch-pazifische Region für Kunden in Ozeanien, Südostasien, Südasien und Ostasien. Alida führt ein aktuelles Verzeichnis der Hosting-Einrichtungen unter https://www.alida.com/trust/legal/ oder einer anderen Seite auf ihrer Website mit demselben Zweck ("**Seite mit den Kundenhinweisen**"). Aus Gründen der Klarheit liegt es im Verhältnis zwischen Alida

und dem Kunden in der Verantwortung des Kunden, alle Vorschriften einzuhalten, die ein Hosting der Kundendaten innerhalb einer bestimmten Gerichtsbarkeit erfordern. Alida unterhält einen globalen Benutzerspeicher, um die Authentifizierung des administrativen Benutzerkontos des Kunden und die Weiterleitung an die entsprechende Hosting-Region wie oben beschrieben zu verwalten. Die Daten in diesem Benutzerspeicher sind in Kanada untergebracht.

8. Zulieferer und Unterauftragsverarbeiter

Alida unterhält mit allen Dienstleistern und Unterauftragsverarbeitern angemessene rechtliche Vereinbarungen, um die Einhaltung der in diesem Anhang festgelegten Verpflichtungen zu gewährleisten, und ist für die Einhaltung der Bedingungen dieses Anhangs durch ihre Dienstleister und Unterauftragsverarbeiter verantwortlich. Alida führt eine aktuelle Liste der Dienstleistern und Unterauftragsverarbeiter und deren Standorte auf der Seite "Mitteilungen für Kunden". Die Kunden können sich registrieren lassen, um automatische Benachrichtigungen über Aktualisierungen der Liste der Dienstleister und Unterauftragsverarbeiter zu erhalten.

9. Löschung und Anonymisierung

Nach Beendigung des Vertrags räumt Alida dem Kunden eine Frist von 30 Tagen ein, um die Daten des Kunden aus der Plattform zu exportieren. Nach Ablauf dieser 30 Tage ist Alida nicht mehr für die Aufbewahrung von Teilnehmerdaten verantwortlich und löscht danach alle in der Plattform gespeicherten Teilnehmerdaten endgültig. Sicherungskopien der Teilnehmerdaten werden 90 Tage danach sicher gelöscht oder überschrieben. Auf Anfrage und sofern verfügbar, bietet Alida dem Kunden die Möglichkeit, bestimmte Felder innerhalb einer Umfrage als persönliche Daten zu kennzeichnen, die nach Ablauf eines vom Kunden festgelegten Zeitraums überschrieben werden sollen. Nur Felder, die mit Mitgliedern verbunden sind, deren Konto auf einen inaktiven Status gesetzt wurde, werden nach Ablauf der vom Kunden festgelegten Zeitspanne überschrieben. Zur Verdeutlichung: Der Datensatz des Mitglieds wird von der Plattform als anonymisiert betrachtet, wenn die vom Kunden angegebenen Felder so überschrieben werden, dass sie keine identifizierenden Daten mehr enthalten; zusätzlich überschreibt die Plattform die E-Mail-Adresse, die Benutzer-ID, den Namen und die Telefonnummer des Mitglieds. Nach dem Überschreiben werden die ursprünglichen Daten für 90 Tage als Backup aufbewahrt. Ungeachtet der vorstehenden Ausführungen löscht Alida die Sicherheits- und Leistungsprotokolldaten bei Beendigung des Abonnements nicht, da diese Daten im Laufe der Zeit aus unserem zentralen Protokollierungssystem überschrieben werden. Die Protokolle enthalten in der Regel keine vom Mitglied zur Verfügung gestellten Daten, obwohl sie in einigen Fällen E-Mail-Adressen, IP-Adressen und andere identifizierende Informationen enthalten können.

10. Kein Verkauf oder Weitergabe von Informationen für kontextübergreifende, verhaltensbezogene Werbung.

Alida akzeptiert oder offenbart keine Kundendaten als Gegenleistung für Zahlungen, Dienstleistungen oder andere Wertgegenstände. Alida verkauft keine Teilnehmerdaten und gibt sie auch nicht weiter, da die Begriffe "verkaufen" und "weitergeben" im California Consumer Privacy Act von 2018 in der jeweils gültigen Fassung, einschließlich des California Privacy Rights Act ("**CCPA**"), definiert sind. Alida verarbeitet die Daten des Kunden nur für die im schriftlichen Vertrag angegebenen Geschäftszwecke. Alida speichert, verwendet oder offenbart keine Kundendaten (a) für kontextübergreifende verhaltensbezogene Werbung oder (b) außerhalb der direkten Geschäftsbeziehung mit dem Kunden. Alida kombiniert keine Teilnehmerdaten mit anderen Daten, wenn und soweit dies mit den Beschränkungen für Dienstleistungsanbieter gemäß CCPA unvereinbar wäre.

11. Persönliche Daten aus dem EWR

In Bezug auf Kundendaten, die als "personenbezogene Daten" der EU-Datenschutzgrundverordnung (DSGVO) oder ähnlichen Gesetzen anderer Länder unterliegen, übernimmt Alida als Datenimporteur, -verarbeiter oder -unterverarbeiter des Kunden die folgenden Verpflichtungen und garantiert, dass Alida

(a) verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des für die Verarbeitung Verantwortlichen, auch im Hinblick auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, es sei denn, der Auftragsverarbeiter ist nach dem Recht der Europäischen Union oder der EU-Mitgliedstaaten, dem er unterliegt, dazu verpflichtet; in einem solchen Fall unterrichtet der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen vor der Verarbeitung über diese rechtliche Verpflichtung, es sei denn, das betreffende Recht verbietet eine solche Unterrichtung aus wichtigen Gründen des öffentlichen Interesses; außerdem unterrichtet der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen unverzüglich, wenn eine Weisung seiner Ansicht nach gegen die DSGVO, nationale Datenschutzgesetze in der EU oder andere geltende Rechtsvorschriften verstößt;

(b) sicherstellt, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verpflichtung zur Vertraulichkeit unterliegen

(c) alle gemäß Artikel 32 der Datenschutz-Grundverordnung (Sicherheit der Verarbeitung) erforderlichen Maßnahmen ergreift;

(d) die in Artikel 28 Absätze 2 und 4 der Datenschutz-Grundverordnung genannten Bedingungen für die Beauftragung eines anderen Auftragsverarbeiters einhält;

(e) unter Berücksichtigung der Art der Verarbeitung den für die Verarbeitung Verantwortlichen durch geeignete technische und organisatorische Maßnahmen unterstützt, soweit dies möglich ist, um die Verpflichtung des für die Verarbeitung Verantwortlichen zur Beantwortung von Anträgen auf Ausübung der in Kapitel III der DSGVO festgelegten Rechte der betroffenen Person zu erfüllen, einschließlich, aber nicht beschränkt auf das Recht auf Auskunft, Berichtigung, Löschung und Übertragbarkeit der personenbezogenen Daten der betroffenen Person; (zur Vermeidung von Zweifeln soll der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen nur dabei unterstützen und in die Lage versetzen, die Verpflichtungen des für die Verarbeitung Verantwortlichen zur Erfüllung der Rechte der betroffenen Personen zu erfüllen, aber der Auftragsverarbeiter soll nicht direkt auf die betroffenen Personen reagieren);

(f) den für die Verarbeitung Verantwortlichen bei der Einhaltung der Verpflichtungen gemäß den Artikeln 32 bis 36 der Datenschutz-Grundverordnung (Sicherheit personenbezogener Daten) unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter vorliegenden Informationen unterstützt;

(g) nach Wahl des für die Verarbeitung Verantwortlichen alle personenbezogenen Daten nach Beendigung der Erbringung von Dienstleistungen im Zusammenhang mit der Verarbeitung löscht oder an den für die Verarbeitung Verantwortlichen zurückgibt und vorhandene Kopien löscht, sofern nicht das Unionsrecht oder das Recht der Mitgliedstaaten die Aufbewahrung der personenbezogenen Daten vorschreibt;

(h) dem für die Verarbeitung Verantwortlichen alle Informationen zur Verfügung stellt, die erforderlich sind, um die Einhaltung der in Artikel 28 der Datenschutz-Grundverordnung festgelegten Verpflichtungen nachzuweisen, und Prüfungen, einschließlich Inspektionen, die von dem für die Verarbeitung Verantwortlichen oder einem anderen von dem für die Verarbeitung Verantwortlichen beauftragten Prüfer durchgeführt werden, zulässt und dazu beiträgt.

12. Bekanntmachung von Änderungen

Von Zeit zu Zeit kann Alida seine Sicherheits- und Datenschutzpraktiken aktualisieren. Alle wesentlichen Änderungen werden mindestens 30 Tage vor ihrem Inkrafttreten auf der Seite "Hinweise für Kunden" veröffentlicht, sofern im Vertrag nichts anderes festgelegt ist. Falls der Kunde feststellt, dass solche wesentlichen Änderungen für ihn nicht akzeptabel sind, kann er seinen Vertrag mit Alida gemäß den Vertragsbedingungen kündigen.

13. Integration

Diese Anlage ist für Alida verbindlich, wenn und soweit sie in einem ordnungsgemäß unterzeichneten Vertrag ausdrücklich vereinbart oder durch Bezugnahme aufgenommen wurde. Dieser Anhang begründet keine Rechte von Drittbegünstigten. Alida akzeptiert oder unterwirft sich keinen zusätzlichen Anforderungen in Bezug auf die Teilnehmerdaten, es sei denn, dies wurde ausdrücklich und schriftlich unter ausdrücklicher Bezugnahme auf den Vertrag und diesen Anhang vereinbart.

Erklärung von Alida zu technischen und organisatorischen Maßnahmen

1. Allgemeines

Diese Erklärung zu den technischen und organisatorischen Maßnahmen beschreibt die Prozesse, die Infrastruktur und die Richtlinien, die Alida zum Schutz ihrer Systeme und der Teilnehmerdaten einsetzt. Großgeschriebene Begriffe haben hier die gleiche Bedeutung wie in der Alida-Datenschutzerklärung.

2. Richtlinien und Verwaltung

Alida hat die folgende Verwaltungsstruktur in Bezug auf ihre Sicherheits- und Datenschutzrichtlinien und Standards (die "**Richtlinien**") eingeführt:

A. Die Richtlinien von Alida wurden von der Geschäftsführung von Alida (die "**Geschäftsführung**") genehmigt;

B. Ein Mitglied der Geschäftsleitung ist für die Sicherheit und den Datenschutz bei Alida verantwortlich und berichtet regelmäßig und erstattet der Geschäftsleitung und dem Vorstand von Alida (der "**Vorstand**") regelmäßig Bericht über diese Angelegenheiten;

C. Die Risiken werden zentral erfasst und bei Bedarf an die Geschäftsleitung und den Vorstand gemeldet;

D. Alida überprüft regelmäßig ihre Richtlinien und die dazugehörige Dokumentation auf ihre Relevanz;

E. Die Nichteinhaltung einer Richtlinie erfordert Genehmigungen in Übereinstimmung mit einem klaren Autorisierungsrahmen;

F. Die Nichteinhaltung von Richtlinien ohne Genehmigung hat Folgen bis hin zu und einschließlich Beendigung des Arbeitsverhältnisses;

G. Alida überprüft regelmäßig seine Richtlinien und die dazugehörigen Unterlagen auf ihre Relevanz

H. Alida führt jedes Jahr Schulungen zum Thema Sicherheit und Datenschutz für die Benutzer durch;

I. Alle Mitarbeiter unterzeichnen die Richtlinien jährlich;

J. Alle neu eingestellten Mitarbeiter von Alida werden, soweit gesetzlich zulässig, auf ihren kriminellen Hintergrund hin überprüft; und

K. Alle Mitarbeiter unterliegen einer schriftlichen Vertraulichkeitsvereinbarung.

3. Sicherheit des Datenzentrums

Alida beherbergt die Plattform in Datenzentren der Enterprise-Klasse, die Folgendes bieten:

A. Unabhängige jährliche Prüfberichte über ihre Sicherheits- und Verfügbarkeitskapazitäten. Solche Berichte sind unter anderem: AICPA's Service Organization Controls ("SOC") Auditberichte oder ISO27001 Zertifizierungen;

B. Redundante Kühlung, Feuerunterdrückung, Stromversorgung und Kommunikation; und

C. 24x7 Wachdienste, physische Zugangskontrolle und Videoüberwachung.

4. Sicherheit der Infrastruktur

Alida hat die folgenden Sicherheitsmechanismen eingeführt:

A. Die Plattform ist durch Firewalls oder funktional gleichwertige Technologien geschützt, die den Datenverkehr auf das beschränken, was für die Bereitstellung des Dienstes erforderlich ist;

B. Der Netzwerkverkehr in das Netzwerk, in dem die Plattform gehostet wird, wird durch Intrusion Detection überwacht;

C. Alle Zugriffe auf die Plattform und ihre unterstützende Infrastruktur werden zentral protokolliert;

D. Automatische 24/7-Überwachung auf bösartige Aktivitäten;

E. Bastion-Hosts und VPN-Zugang mit Zwei-Faktor-Authentifizierung zum Produktionsnetzwerk; und

F. F. Antiviren-Software.

5. Mehrmandantenfähige Umgebung

Alida bietet eine mandantenfähige Plattform, die Daten für mehrere Kunden speichert und die folgenden Schutzmechanismen bietet:

A. Jede Website ist für einen einzigen Kunden bestimmt;

B. Die Websites werden durch ihren Domänennamen und die zugrunde liegende Kontokennung eindeutig identifiziert;

C. Der Zugang zu Websites wird nur den Identitäten gewährt, die direkt mit dem Konto des Kunden verbunden sind;

D. Die Daten werden logisch getrennt, indem entweder separate Datenbankschemata oder Datenattribute verwendet werden, die vom Anwendungscode verwendet werden, um Zugriffsentscheidungen zu treffen; und

E. Detaillierte Infrastrukturprotokolle sind für keinen Kunden zugänglich.

6. Anwendungssicherheit

Alida bietet die folgenden Kontrollen innerhalb und im Umfeld der Plattform:

A. Durch Benutzername und Passwort geschützter Zugang zum Administratorportal und optionale Integration mit SAML 2.0 Identity Providern;

B. Authentifizierter Zugriff auf die Website;

C. Protokollierung der Erstellung / Löschung / Bereitstellung von Studien sowie aller Benutzer-Erstellungen / Änderungen / Löschungen; und

D. Sichere Entwicklungspraktiken und Verwendung von sicheren Softwarebibliotheken. Für die Zwecke dieses Abschnitts ist eine "sichere Softwarebibliothek" eine Bibliothek, die vom Hersteller zur Verfügung gestellt wird, die frei von bekannten Sicherheitsmängeln ist und so konzipiert ist, dass die Entwickler gezwungen sind, die Bibliothek so zu verwenden, dass sie nicht unbeabsichtigt Sicherheitsmängel in die Plattform einbringen.

7. Datenverschlüsselung

A. Alle Verbindungen zur Plattform sind durch verschlüsselte Kanäle geschützt, einschließlich, aber nicht beschränkt auf Transport Layer Security (TLS);

B. Alle Backups sind verschlüsselt; und

C. Alle Systeme, die Teilnehmerdaten speichern, verwenden einen Festplattenspeicher, der im Ruhezustand verschlüsselt ist.

8. Betrieb

A. Alida hat Prozesse wie Schwachstellenmanagement, Reaktion auf Zwischenfälle und Sicherheits-Patching-Verfahren zum Schutz vor bekannten und neuen Bedrohungen eingeführt.

B. Änderungen an Produktionssystemen können nur von autorisierten Systemadministratoren nach einem definierten Qualitätssicherungs-, Änderungsverwaltungs- und Genehmigungsprozess vorgenommen werden.

9. Wiederherstellung im Katastrophenfall und Geschäftskontinuität

A. Alida unterhält vor Ort Momentaufnahmen und Kapazitäten, die ausreichen, um einzelne Websites innerhalb von 48 Stunden wiederherzustellen, wobei der Datenverlust nicht mehr als 24 Stunden betragen darf;

B. Wenn Alida Sicherungskopien der Daten außer Haus schickt, werden diese verschlüsselt und die Schlüssel für die Verschlüsselung bleiben unter der Kontrolle von Alida; und

C. Im Falle eines katastrophalen Ausfalls eines gesamten Rechenzentrums wird Alida alle wirtschaftlich vertretbaren Anstrengungen unternehmen, um die Website des Kunden wiederherzustellen.

10. Datenschutzrichtlinien und Protokolle

A. Alida unterhält Datenschutzrichtlinien, um ihre eigenen internen Praktiken im Hinblick auf die sichere und rechtmäßige Verarbeitung personenbezogener Daten zu regeln. Diese Richtlinien befassen sich mit der Einwilligung, der Einschränkung der Datenerhebung, der Datenqualität, der Einschränkung der Nutzung, der Offenlegung, der Aufbewahrung, der Übermittlung, den Rechten der betroffenen Personen und der Sicherheit, wie sie von den geltenden Datenschutzbestimmungen für die Verarbeitung personenbezogener Daten gefordert wird. "**Anwendbare Datenschutzbestimmungen**" umfassen, sind aber nicht beschränkt auf:

i. Das kanadische Gesetz zum Schutz persönlicher Daten und elektronischer Dokumente ("PIPEDA");

ii. Die Allgemeine Datenschutzverordnung 2016/679 ("DSGVO");

iii. Der Federal Privacy Act 1988 von Australien;

iv. Der Personal Data Protection Act 2012 von Singapur; und

v. Das kalifornische Gesetz zum Schutz der Privatsphäre der Verbraucher ("CCPA").

B. Alida speichert zu Sicherheits- und Überwachungszwecken Protokolle, die persönliche Informationen wie E-Mail-Adressen und IP-Adressen sowie die mit der Plattform durchgeführten Aktionen enthalten.

11. Sicherheitstests

A. Alida führt jährlich einen Penetrationstest der Plattform mit einem von Alida nach eigenem Ermessen bestimmten externen Anbieter durch. Sobald die festgestellten Sicherheitsmängel behoben sind, wird Alida die Behebung bestätigen oder durch einen externen Anbieter bestätigen lassen;

B. Alida wird monatliche Sicherheitsscans der Plattform durchführen;

C. Auf Anfrage des Kunden wird Alida den Nachweis erbringen, dass derartige Penetrationstests und Sicherheitsscans durchgeführt worden sind;

D. Einmal pro Abonnementjahr und mit einer Vorankündigung von mindestens zehn (10) Arbeitstagen kann der Kunde oder sein Vertreter eigene Penetrationstests auf einer von Alida bereitgestellten Website durchführen, die nicht die Website des Kunden ist. Der Kunde stimmt

zu, auf dieses Recht zu verzichten, wenn Alida nach eigenem Ermessen einen gleichwertigen Bericht anbietet, der nicht älter als zwölf (12) Monate ist;

E. Ungeachtet der oben genannten Einschränkungen der Häufigkeit von Penetrationstests sind zusätzliche Tests zur Bestätigung, dass zuvor gemeldete Probleme behoben wurden, in ihrer Häufigkeit nicht begrenzt;

F. Ein Kunde oder sein Bevollmächtigter kann in gegenseitigem Einvernehmen mit den Parteien eine Sicherheitsüberprüfung seiner eigenen Website durchführen, nachdem seine Methodik von Alida geprüft und genehmigt wurde;

G. Solche jährlichen Penetrationstests oder Sicherheitsscans durch den Kunden erfolgen zusätzlich zu den Audit-Rechten, die in der Datenschutzordnung für Kunden von Alida vorgesehen sind;

H. Alida kann die Genehmigung für Penetrationstests oder Sicherheitsscans in angemessener Weise verweigern, wenn Grund zu der Annahme besteht, dass die vom Kunden oder seinem Beauftragten angewandte Methodik die Leistung, Verfügbarkeit oder Integrität der Plattform stört;

I. Wenn Penetrationstests oder Sicherheitsscans durch den Kunden oder seinen Beauftragten die Leistung, Verfügbarkeit oder Integrität der Plattform stören, kann Alida den Kunden anweisen, alle Penetrationstests oder Sicherheitsscans sofort zu stoppen oder zu veranlassen, dass sie gestoppt werden, bis Alida zufrieden ist, dass der Grund für die Störung behoben wurde;

J. Der Kunde wird alle von Alida angemessenerweise angeforderten Informationen über die Art seiner Penetrationstests und Sicherheitsscans zur Verfügung stellen, bevor er mit seiner Arbeit beginnt. Zu diesen Informationen gehören unter anderem: Quell-IP-Adressen, Kontaktinformationen, Namen von Mitarbeitern oder Beauftragten und Zeiten der Tests;

K. Der Kunde oder sein Bevollmächtigter wird die Anweisungen von Alida zur Durchführung von Penetrationstests und Sicherheitsscans befolgen und im Gegenzug wird Alida dem Kunden den notwendigen Zugang zur Durchführung solcher Penetrationstests und Sicherheitsscans gewähren;

L. Wenn der Kunde verlangt, dass festgestellte Sicherheitsmängel behoben werden, muss der Kunde oder sein Bevollmächtigter schriftlich alle Einzelheiten des Sicherheitsmangels mitteilen, so dass Alida das Vorhandensein des Sicherheitsmangels unabhängig bewerten, reproduzieren und überprüfen kann; und

M. Innerhalb von zehn (10) Werktagen, nachdem Alida das Vorhandensein der gemeldeten Sicherheitsmängel bestätigt hat, wird Alida auf Anfrage einen Plan zur Behebung der Mängel gemäß den im folgenden Abschnitt genannten Fristen vorlegen.

12. Behebung von Sicherheitsmängeln

A. Alida verwendet branchenübliche Bewertungsmethoden, wie das Common Weakness Scoring System (CWSS) und das Common Vulnerability Scoring System (CVSS), um den Schweregrad eines festgestellten Sicherheitsmangels zu bewerten. Alida kann diese nach eigenem Ermessen durch gleichwertige Bewertungsmethoden ersetzen.

B. Alida bewertet einen Sicherheitsmangel mit den oben genannten Techniken und kategorisiert die Mängel nach ihrer Auswirkung wie folgt:

Gemeinsame Bezeichnung der Auswirkungen	**CVSS**	**CWSS**
Kritisch	9,0 bis 10,0	90 bis 100
Hoch	7,0 bis 8,9	70 bis 89

Mittel	4,0 bis 6,9	40 bis 69
Niedrig	0,0 bis 3,9	0 bis 39

C. Alida wird Sicherheitsmängel in unserer Plattform nach dem folgenden Zeitplan beheben, sobald der gemeldete Sicherheitsmangel bestätigt ist:

Gemeinsame Bezeichnung der Auswirkungen	**Zeitplan**
Kritisch	Unverzüglich und nicht länger als vierzehn (14) Tage
Hoch	Innerhalb von fünfundvierzig (45) Tagen
Mittel	Innerhalb von neunzig (90) Tagen
Niedrig	Niedrig Innerhalb von einhundertachtzig (180) Tagen

D. Alida kann nach eigenem Ermessen eine vorübergehende Plattform für den Sicherheitsmangel einführen, um die oben genannten Fristen einzuhalten. Solche temporären Plattformen können die vorübergehende Deaktivierung oder Änderung bestimmter Funktionen beinhalten, während an einer dauerhaften Plattform des Sicherheitsmangels gearbeitet wird. Sollte Alida sich dazu entschließen, Funktionen vorübergehend zu deaktivieren oder zu ändern, um einen Sicherheitsmangel zu beheben, wird der Kunde diese Maßnahmen nicht als eine Einschränkung des Dienstes betrachten;

E. Alida kann die Behebung eines gemeldeten Sicherheitsmangels in angemessener Weise aufschieben, unter anderem aus folgenden Gründen:

   a. Der Sicherheitsmangel wird zu spät im aktuellen Release-Zyklus gemeldet, um ihn im Rahmen unserer Änderungsmanagement-Praktiken sicher zu berücksichtigen;

   b. Eine geplante Änderung oder Korrektur wird den Sicherheitsmangel in einem angemessenen Zeitrahmen beheben; oder

   c. Alle verfügbaren Ressourcen arbeiten bereits an einem Sicherheitsmangel von größerer Tragweite.

F. Alida kann die Behebung eines Sicherheitsmangels nach billigem Ermessen ablehnen, wenn der Sicherheitsmangel keinen angemessenen Weg bietet, um Zugang zu den Daten des Kunden oder der Plattform zu erhalten.