Auftragsverarbeitungsvertrag

Zuletzt aktualisiert am: 07.01.2025

Der vorliegende Auftragsverarbeitungsvertrag (nachfolgend der „AVV“ bzw. der „Vertrag“ genannt) bildet den Bestandteil der zwischen dem Administrator des Bitrix24 Kundenaccounts und Alaio getroffenen Vereinbarung (https://www.bitrix24.de/terms/) über die Bereitstellung von Services des Auftragsverarbeiters (gemäß der jeweils gültigen Definition) sowie über die Verarbeitung personenbezogener Daten des Nutzers des Bitrix24 Kundenaccounts in Übereinstimmung mit den geltenden

Der vorliegende Auftragsdatenverarbeitungsvertrag ist ab dem Datum seines Inkrafttretens wirksam.

Wenn Sie dem Auftragsverarbeitungsvertrag im Namen des Kunden zustimmen, sichern Sie zu, dass Sie: a) rechtlich vollumfänglich befugt sind, den Kunden an diesen Auftragsverarbeitungsvertrag rechtlich zu binden, (b) diesen Auftragsverarbeitungsvertrag gelesen und verstanden haben und (c) im Namen des Kunden diesem Auftragsverarbeitungsvertrag zustimmen. Wenn Sie keine rechtlichen Befugnisse haben, den Kunden rechtlich zu binden, sollen Sie diesem Auftragsverarbeitungsvertrag nicht zustimmen.

GELTUNGSBEREICH DIESES AUFTRAGSDATENVERARBEITUNGSVERTRAGES

Bei Widersprüchen zwischen den Bestimmungen dieses Auftragsverarbeitungsvertrages und den Nutzungsbedingungen (https://www.bitrix24.eu/terms/) hat der Auftragsverarbeitungsvertrag Vorrang. Sofern die Nutzungsbedingungen nicht durch die Bestimmungen dieses Vertrages geändert werden, bleiben sie im vollen Umfang wirksam.

DIE PARTEIEN VEREINBAREN HIERMIT WAS FOLGT:

1. PRÄAMBEL

Dieser AVV legt die von den Parteien getroffenen Vereinbarungen in Bezug auf die Verarbeitung und die Sicherheit personenbezogener Daten des Kunden in Übereinstimmung mit den Datenschutzvorschriften fest.

1.1 DEFINITIONEN UND AUSLEGUNG:

“Alaio” hat die Bedeutung gemäß dem Abschnitt "Vertragspartei" der Nutzungsbedingungen (https://bitrix24.com/terms/) von Alaio (ehemals Bitrix24), abhängig von der Registrierung der Domainzone Ihres Kundenaccounts, sind die folgenden juristischen Personen Ihre Datenverantwortlichen:
a) Alaio Cloud Limited, ein nach dem Recht der Republik Zypern eingetragenes Unternehmen mit Sitz in Frema House, Büro 102, Nr. 9, Constantinou Paparigopoulou Str., 3106, Limassol, Zypern;
b) Alaio Inc., ein Unternehmen, das nach dem Recht des Commonwealth of Virginia, Vereinigte Staaten von Amerika, organisiert ist, mit eingetragener Adresse in 700 North Fairfax St., Suite 614-B, Alexandria, VA 22314, USA; und

c) Bitrix24 India Private Limited mit eingetragenem Firmensitz in B-01, Prestige Centre Point, Edward Road, H.K.P.Road, Bangalore, Bangalore North, Karnataka, Indien, 560054, und seine verbundenen Unternehmen.

(zusammen "Alaio", "Wir", "Uns", "Unser" oder "Bitrix24").

“Administrator” bezieht sich auf einen Nutzer mit administrativen Privilegien, wie in den Nutzungsbedingungen definiert (https://www.bitrix24.de/terms/).

"Bitrix24" bedeutet; Bitrix24 Website, Produkte und Dienste, die von Alaio gemäß den Bitrix24 Nutzungsbedingungen (https://www.bitrix24.com/terms/) bereitgestellt werden.

„Personenbezogene Daten des Kunden” bezieht sich auf alle personenbezogenen Daten, die von Alaio im Auftrag des Administrators im Rahmen der Bereitstellung der Services des Auftragsverarbeiters durch Alaio verarbeitet werden.

„**Verletzung des Schutzes personenbezogener Daten**” bezieht sich auf eine Sicherheitsverletzung bei Bitrix24, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten des Kunden in den von Alaio verwalteten oder auf eine andere Weise kontrollierten Systemen führt. „Verletzung des Schutzes personenbezogener Daten” bezieht sich nicht auf fehlgeschlagene Versuche oder Aktivitäten, welche die Sicherheit personenbezogener Daten des Kunden nicht gefährden, darunter erfolglose Anmeldeversuche, Pings, Port-Scans, Denial-of-service-Angriffe und sonstige Angriffe auf Netzwerke, Firewalls oder Netzwerksysteme.

"Datenschutzgesetzgebung" bezeichnet alle Gesetze und Vorschriften, die von Zeit zu Zeit geltende Anforderungen in Bezug auf die Verwendung personenbezogener Daten und die Privatsphäre der elektronischen Kommunikation, einschließlich, aber nicht beschränkt auf: EU 2016/679 Datenschutz-Grundverordnung (DSGVO); California Privacy Rights Act von 2020 und alle anderen anwendbaren Datenschutzgesetze des Bundes und der Bundesstaaten in den USA; Allgemeines Datenschutzgesetz (Gesetz Nr. 13.709/2018 von Brasilien, (Lei Geral de Proteção de Dados); Gesetz Nr. 30 von 2018 über den Schutz personenbezogener Daten von Bahrein; der Federal Privacy Act 1988 von Australien; Gesetz zum Schutz personenbezogener Daten und elektronischer Dokumente von Kanada; Das chinesische Gesetz zum Schutz personenbezogener Daten; Verordnung über personenbezogene Daten (Datenschutz) (Kap. 486) von Hongkong; Information Technology Act 2000 in der durch den Information Technology (Amendment) Act 2008 von Indien geänderten Fassung; Gesetz zum Schutz digitaler personenbezogener Daten von Indien; Gesetz Nr. 11 von 2008 über elektronische Informationen und Transaktionen (EIT-Gesetz) von Indonesien; Regierungsverordnung Nr. 71 von 2019 über die Bereitstellung elektronischer Systeme und Transaktionen (Verordnung über elektronische Systeme) von Indonesien; Verordnung Nr. 20 von 2016 des Ministeriums für Kommunikation und Informationstechnologie (MCI) über den Schutz personenbezogener Daten in einem elektronischen System (Verordnung über personenbezogene Daten) von Indonesien; Gesetz zum Schutz der Privatsphäre (5741-1981) Israels; Gesetz über den Schutz personenbezogener Daten von Japan; Gesetz zum Schutz personenbezogener Daten von 2010 (PDPA von Malaysia; Privacy Act 1993 von Neuseeland; Das Datenschutzgesetz von 2012 (Republic Act Nr. 10173) der Philippinen; Gesetz Nr. 13 von 2016 zum Schutz der Privatsphäre personenbezogener Daten von Katar; Das Gesetz zum Schutz personenbezogener Daten von 2012 von Singapur; Das Gesetz zum Schutz personenbezogener Daten von 2013 in Südafrika; Gesetz zum Schutz personenbezogener Daten von Südkorea; Bundesgesetz über den Datenschutz vom 19. Juni 1992 (Schweiz), Gesetz über den Schutz personenbezogener Daten von Taiwan; Gesetz über den Schutz personenbezogener Daten Nr. 6698 der Türkei; Gesetz Nr. 18.331 über den Schutz personenbezogener Daten und Habeas-Daten-Klagen, geändert durch die Gesetze Nr. 18.719 und 18.996 von Uruguay; Dekret Nr. 414/009 zur Regelung der PDPL von Uruguay.

„Datum des Inkrafttretens“ bezieht sich jeweils entsprechend auf: das Datum, an dem der Kunde auf „Akzeptieren” geklickt hat oder die Parteien anderweitig diesem Auftragsverarbeitungsvertrag zugestimmt haben.

„E-Mail-Adresse für Benachrichtigungen” bezieht sich auf die E-Mail-Adresse, die der erste Administrator für die Registrierung des Portals verwendet hat, und die außerdem genutzt wird, um bestimmte Benachrichtigungen von Bitrix24 im Zusammenhang mit diesen Auftragsverarbeitungsbedingungen zu erhalten, oder die zum Zwecke der E-Mail-Authentifizierung genutzt wird.

„Personenbezogene Daten” bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen; als identifizierbar wird

eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

„Verarbeitung personenbezogener Daten“ bedeutet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (wobei „Verarbeitung” „Verarbeitungsvorgänge” und „verarbeitet” die gleiche Bedeutung haben).

„Sicherheitsmaßnahmen“ bezieht sich auf die Maßnahmen zum Schutz personenbezogener Daten gegen eine unbeabsichtigte oder unrechtmäßige Vernichtung, unbeabsichtigten Verlust, eine Veränderung oder unbefugte Offenlegung beziehungsweise gegen einen unbefugten Zugang zu personenbezogenen Daten oder gegen alle anderen Formen unrechtmäßiger Verarbeitung gemäß der Beschreibung in der jeweils gültigen Fassung des über den Link im Anhang 2 zu diesem AVV abrufbaren Dokuments (beziehungsweise dessen maßgeblichen Teils, je nachdem welche Services der Administrator von Bitrix24 erwirbt).

„Services des Auftragsverarbeiters” bezieht sich auf die Erbringung von Wartungs- und Supportleistungen sowie Beratungs- und professionellen Dienstleistungen, auf die Breitstellung von Software als Dienst (Software as a Service) und alle anderen nach dem Vertrag zu erbringenden Leistungen, in Rahmen derer Bitrix24 personenbezogene Daten im Namen von dem Administrator verarbeitet.

„Unterauftragsverarbeiter” bezieht sich auf Dritte, die von Bitrix24 zum Zwecke der Bereitstellung bestimmter Services des Auftragsverarbeiters und der damit verbundenen technischen Unterstützung einen logischen Zugang zu personenbezogenen Daten erhalten und zu ihren Verarbeitung ermächtigt werden.

„Vertragslaufzeit” bezieht sich auf den Zeitraum zwischen dem Datum des Inkrafttretens und der Beendigung der Bereitstellung der Services des Auftragsverarbeiters an den Administrator durch Bitrix24.

“Nutzer” bezieht sich auf einen beliebigen Nutzer des Bitrix24 Kundenaccounts mit administrativen Privilegien oder ohne diese, wie in den Nutzungsbedingungen definiert (https://www.bitrix24.de/terms/).

Die in diesem AVV verwendeten Begriffe **„Verantwortlicher”**, **„betroffene Person”**, **„personenbezogene Daten”**, **„Verarbeitung”**, **„Auftragsverarbeiter”** und

„Aufsichtsbehörde” haben die ihnen in der DSGVO zugewiesene Bedeutung.

2. VERARBEITUNG VON PERSONENBEZOGENEN DATEN

2.1 Verantwortlichkeiten und Einhaltung gesetzlicher Vorschriften; Genehmigung.

2.1.1 Pflichten des Auftragsverarbeiters und des Verantwortlichen. Die Parteien sind sich einig und erklären sich damit einverstanden, dass:

(a) Im Anhang 1 zu den Standardvertragsklauseln der Gegenstand und die Einzelheiten zu der Verarbeitung personenbezogener Daten festgelegt sind;

(b) Alaio in Bezug auf personenbezogene Daten der Auftragsverarbeiter gemäß den Datenschutzvorschriften ist;

(c) Der Administrator in Bezug auf personenbezogene Daten der Verantwortliche oder gegebenenfalls Auftragsverarbeiter gemäß den Datenschutzvorschriften ist;

(d) Jede Partei verpflichtet ist, die ihr gemäß den Datenschutzvorschriften obliegenden Pflichten hinsichtlich der Verarbeitung personenbezogener Daten zu erfüllen;

(e) Der Administrator verpflichtet ist, personenbezogene Daten im Rahmen seiner Nutzung oder Inanspruchnahme der Services in Übereinstimmung mit den in den Datenschutzvorschriften festgelegten Anforderungen zu verarbeiten. Der Administrator gewährleistet ferner, dass die von ihm mit der Verarbeitung personenbezogener Daten beauftragten Unterauftragsverarbeiter die Datenschutzvorschriften einhalten. Der Administrator trägt die alleinige Verantwortung für die Genauigkeit, Qualität und Rechtmäßigkeit personenbezogener Daten und der für die Erhebung personenbezogener Daten eingesetzten Mittel. Alaio wird den Administrator unverzüglich informieren, wenn es der Ansicht ist, dass eine Datenverarbeitungsanweisung gegen die DSGVO oder andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

2.2 Genehmigung durch externe Verantwortliche. Wenn der Administrator der Auftragsverarbeiter ist, sichert der Administrator gegenüber Alaio zu, dass seine Handlungen, welche die personenbezogenen Daten betreffen, und die beauftragten Unterauftragsverarbeiter, darunter die Beauftragung von Alaio als einen weiteren Auftragsverarbeiter, von dem entsprechenden Verantwortlichen genehmigt worden sind.

2.3 Die Parteien sind sich einig, dass Alaio beziehungsweise die Unternehmen der Alaio Guppe verpflichtet sind, bei der Beauftragung von Unterauftragsverarbeitern die im nachstehenden Abschnitt 7 „Unterauftragsverarbeiter” festgelegten Anforderungen einzuhalten.

2.4 Durch den Abschluss dieses Auftragsverarbeitungsvertrages weist der Administrator Alaio an, personenbezogene Daten ausschließlich in Übereinstimmung mit den geltenden gesetzlichen Vorschriften zu bearbeiten: (a) um Services des

Auftragsverarbeiters bereitzustellen und die damit verbundene technische Unterstützung zu leisten; (b) wie im Rahmen der Nutzung der Services des Auftragsverarbeiters durch den Administrator (einschließlich in den Einstellungen und anderen Funktionen der Services des Auftragsverarbeiters) sowie der damit verbundenen technischen Unterstützung weiter festgelegt; (c) wie in diesem Auftragsverarbeitungsvertrag bestimmt und (d) wie in den schriftlichen Anweisungen des Administrators, die von Bitrix24 zum Zwecke dieses Auftragsverarbeitungsvertrages als maßgebliche Anweisungen akzeptiert wurden, näher dokumentiert.

2.5.Löschung nach Ablauf der Vertragslaufzeit. Nach Ablauf der Vertragslaufzeit weist der Administrator Alaio an, alle personenbezogenen Daten (einschließlich vorhandener Kopien) aus den Systemen von Bitrix24 in Übereinstimmung mit geltendem Recht zu löschen. Alaio wird dieser Anweisung so schnell wie möglich und innerhalb eines Zeitraums von maximal 90 Tagen nachkommen, es sei denn, ein geltendes Gesetz erfordert eine Speicherung.

2.5.1 Löschung des Accounts

Kostenpflichtige Pläne gehen gemäß dem oben beschriebenen Prozess in den kostenlosen Plan über.
Bleibt eine Instanz des Bitrix24 Kundenaccounts, welche auf einem kostenlosen Tarif läuft (egal, ob darauf zurückgesetzt oder ursprünglich kostenlos erstellt), im Laufe von 30 Tagen inaktiv, wird sie archiviert, und kann nur durch einen Administrator wiederhergestellt werden (es muss also ein Nutzer mit den administrativen Zugriffsrechten sein).

Zur Wiederherstellung des Accounts reicht, dass ein Nutzer sich einloggt.

Wird sich kein Nutzer im Laufe von weiteren 15 Tagen einloggen, nachdem die Instanz archiviert wurde, wird die Instanz des Bitrix24 Kundenaccounts komplett gelöscht.

2.5.2 Der Administrator kann die Löschung des Bitrix24 Kundenaccounts veranlassen, indem er zunächst andere Administratoren, falls vorhanden, deaktiviert, was die Löschung aller verbundenen Nutzeraccounts und aller verbundenen Nutzerinhalte zur Folge hat, vorbehaltlich der Verfügbarkeit einer solchen Funktion. In diesem Fall wird der Bitrix24 Kundenaccount sofort inaktiv gemacht und im Laufe von 90 (neunzig) Kalendertagen vollständig gelöscht. Dieser Vorgang löscht jedoch nicht vollständig die Bitrix24 Network-Accounts der Nutzer, die für die Verwendung in anderen Bitrix24 Kundenaccounts aktiv bleiben.

3. LAUFZEIT DIESES AVV

Dieser AVV ist ab dem Datum des Inkrafttretens wirksam und bleibt ungeachtet des Ablaufs der Vertragslaufzeit weiterhin gültig, bis alle personenbezogenen Daten des Kunden durch Bitrix24 wie in diesem AVV festgelegt gelöscht werden. Die Löschung der Daten bewirkt eine automatische Beendigung des AVV.

4. RECHTE BETROFFENER PERSONEN

4.1 Wenn der Administrator im Rahmen seiner Nutzung oder Inanspruchnahme der Services keine Möglichkeit zur Berichtigung, Korrektur, Einschränkung oder Löschung personenbezogener Daten, wie in den Datenschutzvorschriften festgelegt, hat, ist Alaio (unter Berücksichtigung der Verarbeitungsart personenbezogener Daten und gegebenenfalls gemäß Artikel 11 der DSGVO) verpflichtet, durch die Bereitstellung entsprechender Funktionen im Rahmen der Services des Auftragsverarbeiters den Administrator dabei zu unterstützen, dessen Pflicht zur Beantwortung von Anträgen betroffener Personen nachzukommen. Dies umfasst gegebenenfalls auch die Pflicht des Administrators zur Beantwortung von Anträgen im Rahmen der Wahrnehmung von in Kapitel III der DSGVO festgelegten Rechten oder anderen Datenschutzgesetzen durch betroffene Personen.

4.2 Alaio ist verpflichtet, den Administrator in dem gesetzlich zulässigen Umfang über die von betroffenen Personen gestellten Anträge auf Zugang zu, Berichtigung, Korrektur, Einschränkung und Löschung personenbezogener Daten dieser Personen beziehungsweise auf Wahrnehmung sonstiger in der DSGVO oder in den anderen Datenschutzgesetzen vorgesehenen Rechte umgehend zu informieren. Alaio ist nicht berechtigt, Anträge betroffener Personen ohne eine schriftliche Einwilligung des Administrators zu beantworten. Dies gilt nicht für eine Bestätigung, dass der Antrag den Administrator betrifft. Alaio kooperiert mit dem Administrator und unterstützt ihn bei der Beantwortung von Anträgen betroffener Personen auf Zugang zu deren personenbezogenen Daten beziehungsweise auf Wahrnehmung sonstiger Rechte gemäß der DSGVO oder den anderen Datenschutzgesetzen, sofern dies rechtlich zulässig ist und sofern der Administrator im Rahmen seiner Nutzung oder Inanspruchnahme der Services keinen Zugang zu diesen personenbezogenen Daten hat.

5. MITARBEITER

5.1 Alaio stellt sicher, dass ihre an der Verarbeitung personenbezogener Daten beteiligten Mitarbeiter über den vertraulichen Charakter personenbezogener Daten informiert sind, eine entsprechende Schulung zu ihren Aufgaben erhalten haben und den Geheimhaltungspflichten in dem im Anhang zu diesem AVV festgelegten Umfang unterliegen, wobei diese Pflichten auch nach der Beendigung der Beschäftigung dieser
Personen bei Alaio fortbestehen.

5.2 Alaio stellt sicher, dass der Zugang der Unternehmen der Alaio Gruppe zu personenbezogenen Daten ausschließlich denjenigen Beschäftigten vorbehalten ist, die einen solchen Zugang zum Zwecke der Vertragserfüllung benötigen.

6. DATENSICHERHEIT

6.1 Alaio bietet administrative, technische und organisatorische Garantien zum Schutz der Sicherheit, Vertraulichkeit und Integrität personenbezogener Daten. Diese Maßnahmen sind im Anhang 2 zu diesem AVV beschrieben.

6.2 Sicherheitsmaßnahmen bei Alaio. Alaio ist verpflichtet, die im Anhang 2 zu diesem AVV beschriebenen technischen, physischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten gegen eine unbeabsichtigte oder unrechtmäßige Vernichtung, einen unbeabsichtigten oder unrechtmäßigen Verlust, eine unbeabsichtigte oder unrechtmäßige Veränderung oder unbefugte Offenlegung beziehungsweise gegen einen unbefugten Zugang umzusetzen und aufrechtzuerhalten.

Die Sicherheitsmaßnahmen gemäß Anhang 2 zu diesem AVV umfassen unter anderem die Maßnahmen: (a) zur Sicherstellung fortlaufender Vertraulichkeit, Integrität, Verfügbarkeit und Stabilität von Systemen und Services von Bitrix24; (b) zur raschen Wiederherstellung des Zugangs zu personenbezogenen Daten bei einer Verletzung des Schutzes personenbezogener Daten sowie (c) zur regelmäßigen Wirksamkeitsüberprüfungen. Alaio ist berechtigt, die Sicherheitsmaßnahmen von Zeit zu Zeit zu verbessern oder zu ändern, vorausgesetzt, dass solche Verbesserungen und Änderungen zu keiner Verschlechterung der allgemeinen Sicherheit der Services des Auftragsverarbeiters führen.

6.3 Befolgung von Sicherheitsmaßnahmen durch die Mitarbeiter von Alaio. Alaio trifft angemessene Vorkehrungen zur Sicherstellung der Befolgung von Sicherheitsmaßnahmen durch ihre Mitarbeiter, Auftragnehmer und Unterauftragsverarbeiter in dem für ihren Tätigkeitsbereich angemessenen Umfang. Dies beinhaltet, dass alle zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder im entsprechenden Umfang gesetzlicher Verpflichtung zur Vertraulichkeit gemäß der Beschreibung im Anhang 2 zu diesem AVV unterliegen.

6.4 Unterstützung durch Alaio bei Sicherheitsmaßnahmen. Der Administrator erklärt sich damit einverstanden, dass Alaio den Administrator bei der Einhaltung von Pflichten des Nutzers betreffend die Sicherheit personenbezogener Daten und betreffend Verletzungen des Schutzes personenbezogener Daten, unter anderem gegebenenfalls von Pflichten des Kunden gemäß Artikel 32 bis einschließlich Artikel 34 der DSGVO unterstützt, indem sie:

(a) die Sicherheitsmaßnahmen in Übereinstimmung mit dem Anhang 2 zu diesem AVV umsetzt und aufrechterhält;

(b) die Bestimmungen des Abschnitts 5 (Verletzungen des Schutzes personenbezogener Daten) einhält und

(c) dem Kunden die Sicherheitsdokumentation zur Verfügung stellt.

7. UNTERAUFTRAGSVERARBEITER

7.1 Zustimmung zur Beauftragung von Unterauftragsverarbeitern. Der Administrator gestattet Alaio ausdrücklich die Beauftragung externer Unterauftragnehmer im Zusammenhang mit der Bereitstellung von Services (abrufbar auch unter Alaio Infrastruktur und Unterauftragsverarbeiter).

7.2 Anforderungen an die Beauftragung von Unterauftragsverarbeitern. Bei der Beauftragung von Unterauftragsverarbeitern verpflichtet sich Alaio:

(a) anhand einer schriftlichen Vereinbarung sicherzustellen, dass:

(i) der Unterauftragsverarbeiter ausschließlich dann auf die personenbezogenen Daten zugreifen und diese nutzen kann, wenn dies zur Erfüllung der ihm im Rahmen des Unterauftrages übertragenen Pflichten erforderlich ist, und sich dabei an die Nutzungsbedingungen (einschließlich dieses AVV) hält;

(ii) der Unterauftragsverarbeiter den in Artikel 28(3) der DSGVO festgelegten Datenschutzbestimmungen unterliegt, wenn die Verarbeitung personenbezogener Daten in den Anwendungsbereich der DSGVO fällt;

(b) für die Einhaltung aller im Rahmen des Unterauftrages dem Unterauftragsverarbeiter übertragenen Pflichten sowie für alle dessen Handlungen und unterlassenen Handlungen im vollen Umfang zu haften.

(c) in vollem Umfang für alle Verpflichtungen zu haften, die an den Unterauftragsverarbeiter vergeben werden, sowie für alle Handlungen und Unterlassungen des Unterauftragsverarbeiters.

7.3 Widerspruchsrecht gegen Beauftragung neuer Unterauftragsverarbeiter.

Im Falle einer Beauftragung neuer Unterauftragsverarbeiter während der Vertragslaufzeit und sofern die DSGVO auf die Verarbeitung personenbezogener Daten Anwendung findet, verpflichtet sich Alaio, den Administrator spätestens 10 Tage bevor der neue Unterauftragsverarbeiter mit der Verarbeitung personenbezogene Daten beginnt, über die Beauftragung (mit Angabe zu der Firma und dem Sitz des entsprechenden Unterauftragsverarbeiters sowie zu den von ihm zu erbringenden Leistungen) zu benachrichtigen, indem er eine E-Mail an die E-Mail-Adresse für Benachrichtigungen versendet.

Der Administrator kann der Beauftragung eines neuen Unterauftragsverarbeiters widersprechen, indem er Alaio innerhalb von fünf (5) Werktagen nach dem Erhalt einer von Alaio versandten Mitteilung umgehend schriftlich benachrichtigt. Sollte der Administrator der Beauftragung eines neuen Unterauftragsverarbeiters widersprechen, wird Alaio angemessene Anstrengungen unternehmen, um dem Administrator geänderte Services zur Verfügung zu stellen oder eine wirtschaftlich vertretbare Änderung der Konfiguration oder der Nutzung der Services durch den Kunden zu empfehlen, bei der keine Verarbeitung personenbezogener Daten durch den abgelehnten neuen Unterauftragsverarbeiter stattfindet. Dies darf jedoch nicht dazu führen, dass der Kunde dadurch unverhältnismäßig benachteiligt wird. Ist Alaio nicht in der Lage, eine solche Änderung innerhalb eines angemessenen Zeitraums, spätestens jedoch innerhalb von dreißig (30) Tagen zu bewirken, kann der Administrator den entsprechenden Auftrag mittels einer schriftlichen Mitteilung an

Alaio stornieren. Dies gilt ausschließlich für diejenigen Services, die von Alaio nur mit Hinzuziehung des abgelehnten neuen Unterauftragsverarbeiters bereitgestellt werden können. Alaio erstattet dem Administrator alle vorausbezahlten Gebühren für die stornierten Services für die verbleibende Laufzeit des Auftrages ab der Wirksamkeit der Stornierung, ohne dass der Administrator eine Vertragsstrafe für eine solche Stornierung zahlen muss.

8. VERLETZUNGEN DES SCHUTZES PERSONENBEZOGENER DATEN.

8.1 Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten. Sollte Alaio Kenntnis von einer Verletzung des Schutzes personenbezogener Daten erlangen, ist Alaio verpflichtet: (a) den Administrator über die Verletzung des Schutzes personenbezogener Daten umgehend zu benachrichtigen, und (b) angemessene

Maßnahmen zur Minimierung der Schäden und zum Schutz personenbezogener Daten unverzüglich zu ergreifen.

8.2 Angaben zu einer Verletzung des Schutzes personenbezogener Daten. Eine Benachrichtigung hat, sofern möglich, Einzelheiten zu der Verletzung des Schutzes personenbezogener Daten zu enthalten. Dies umfasst unter anderem die Maßnahmen zur Minimierung etwaiger Risiken und die Empfehlungen von Alaio an den Administrator zum Umgang mit der Verletzung des Schutzes personenbezogener Daten.

8.3 Übersendung der Benachrichtigung. Alaio nimmt die Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten an die E-Mail-Adresse für

Benachrichtigungen oder nach eigenem Ermessen von Bitrix24 (unter anderem wenn der Kunde keine E-Mail-Adresse angegeben hat) auf einem anderen direkten

Kommunikationsweg (z.B. telefonisch oder bei einem persönlichen Gespräch) vor. Die Pflicht zur Angabe der E-Mail-Adresse für Benachrichtigungen obliegt alleine dem Administrator und er hat sicherzustellen, dass die E-Mail-Adresse für Benachrichtigungen aktuell und gültig ist.

8.4 Pflicht zur Benachrichtigung Dritter. Der Administrator trägt die alleinige Verantwortung für die

Einhaltung der für den Administrator geltenden gesetzlichen Bestimmungen betreffend die Benachrichtigungspflicht sowie für die Einhaltung von Pflichten zur Benachrichtigung Dritter im Zusammenhang mit etwaigen Verletzungen des Schutzes personenbezogener Daten.

8.5 Keine Schuldanerkenntnis seitens Alaio. Eine Benachrichtigung über oder eine Reaktion auf eine Verletzung des Schutzes personenbezogener Daten seitens Alaio gilt nicht als eine Schuldanerkenntnis oder Anerkennung einer Haftung seitens Alaio in Bezug auf die Verletzung des Schutzes personenbezogener Daten.

9. ÜBERPRÜFUNG DER EINHALTUNG DES AVV

9.1 Um die Einhaltung ihrer Pflichten aus diesem AVV durch Alaio nachzuweisen, sowie auf Anfrage des Administrators ist Alaio verpflichtet, ausführlichere

Informationen über die im Anhang 2 zu diesem AVV beschriebenen Sicherheitsmaßnahmen bereitzustellen.

9.2 Auf Anfrage des Administrators und vorbehaltlich der in diesem AVV festgelegten Vertraulichkeitspflichten ist Alaio verpflichtet, dem Kunden, bei dem es sich um keinen Wettbewerber von Alaio handelt (bzw. einem unabhängigen externen Prüfer des Administrators, bei dem es sich um keinen Wettbewerber von Alaio handelt) Informationen bezüglich der Einhaltung der in diesem AVV festgelegten Pflichten und der Umsetzung der im Anhang 2 zu diesem AVV angeführten Sicherheitsmaßnahmen vorzulegen. Der Administrator kann bei Alaio eine Vor-Ort-Überprüfung der für den Schutz personenbezogener Daten maßgeblichen Architektur, Systeme und Verfahren an Standorten, an denen personenbezogene Daten gespeichert werden, beantragen. Der Administrator ist verpflichtet, Alaio die von Alaio oder von ihren Unterauftragsverarbeitern für solche Vor-Ort-Überprüfungen aufgewendete Zeit zu vergüten. Die Vergütung richtet sich nach den bei Alaio geltenden Sätzen für professionelle Dienstleistungen, die dem Administrator auf Anfrage vorgelegt werden. Vor dem Beginn einer solchen Vor-Ort-Überprüfung bestimmen der Administrator und Alaio im beiderseitigen Einvernehmen neben dem von dem Administrator zu zahlenden Erstattungssatz den Umfang, den Zeitpunkt und die Dauer der jeweiligen Überprüfung. Alle Erstattungssätze müssen angemessen sein und die von Alaio oder ihren externen Unterauftragsverarbeitern aufgewendeten Ressourcen berücksichtigen. Der Administrator benachrichtigt Alaio unverzüglich über etwaige im Rahmen einer Überprüfung festgestellte Verstöße.

10. DATENSCHUTZ-FOLGEABSCHÄTZUNG

Auf Anfrage des Administrators unterstützt Alaio den Administrator bei der Sicherstellung der Einhaltung aller Pflichten des Administrators in Bezug auf Datenschutz-Folgeabschätzungen und die vorherige Konsultation, einschließlich (gegebenenfalls) der Pflichten des Administrators gemäß Artikeln 35 und 36 der DSGVO, sofern der Kunde anderweitig keinen Zugang zu den maßgeblichen Informationen hat und sofern solche Informationen Alaio vorliegen. Alaio bietet dem Administrator angemessene Unterstützung bei der Zusammenarbeit mit der Aufsichtsbehörde bei der Erfüllung deren Aufgaben an.

11. DATENÜBERMITTLUNGEN

11.1 Geografie der Dateispeicherung abhängig von den Alaio (Bitrix24) Domainzonen wird im Bereich Alaio Infrastruktur und Unterauftragsverarbeiter beschrieben. Alle über die Domainzonen Bitrix24.eu, Bitrix24.de, Bitrix.it, Bitrix24.pl, Bitrix24.uk und Bitrix24.fr erhobenen Daten werden durch Alaio Cloud Limited, die ihren Sitz in der Republik Zypern hat, innerhalb des Europäischen Wirtschaftsraums verarbeitet und in der Europäischen Union, nämlich in Frankfurt, Deutschland, in den Datenzentren von Amazon Web Services gehostet. Diese

Datenzentren entsprechen im vollen Umfang den Bestimmungen der DSGVO - https://aws.amazon.com/blogs/security/...dpr-ready/

11.2 Weitere Informationen über die Datenverarbeitungsvorgänge betreffend die über die Domainnamen Bitrix24.com, Bitrix24.com.br, Bitrix24.in, Bitrix24.tr, Bitrix24.cn, Bitrix24.cn/tc, Bitrix24.mx , Bitrix24.co, Bitrix24.vn, Bitrix24.id, Bitrix24.jp, Bitrix24.com/my, Bitrix24.com/th, Bitrix24.com.tr registrierten Kunden entnehmen Sie bitte dem Bereich Alaio Infrastruktur und Unterauftragsverarbeiter.

11.3 Internationale Datenübermittlungen.

11.3.1 Alaio kann personenbezogene Daten von Nutzern in der Russischen Föderation vorbehaltlich angemessener Garantien gemäß Artikel 46 DSGVO (siehe Anhang 11.4) und in den USA (siehe Anhang 11.3.2 und 11.3.3) verarbeiten.

11.3.2 Speziell für Datenübertragungen aus der EU, dem Vereinigten Königreich und der Schweiz in die USA hält sich Alaio, Inc. an das EU-U.S. Data Privacy Framework (EU-U.S. DPF), die britische Erweiterung des EU-U.S. DPF und das Swiss-U.S. Datenschutzrahmenwerk (Swiss-U.S. DPF), wie vom US-Handelsministerium festgelegt. Alaio, Inc. hat dem US-Handelsministerium bescheinigt, dass es die Grundsätze des EU-US-Datenschutzrahmens (EU-U.S. DPF-Grundsätze) in Bezug auf die Verarbeitung personenbezogener Daten einhält, die von der Europäischen Union im Vertrauen auf den EU-U.S. DPF und vom Vereinigten Königreich (und Gibraltar) unter Berufung auf die britische Erweiterung des EU-U.S. DPF erhalten werden. Alaio, Inc. hat dem US-Handelsministerium bescheinigt, dass es sich an das Swiss-U.S. Grundsätze des Datenschutzrahmens (Swiss-U.S. DPF-Grundsätze) in Bezug auf die Verarbeitung personenbezogener Daten, die aus der Schweiz im Vertrauen auf das Swiss-U.S. DPF. Im Falle eines Widerspruchs zwischen den Bestimmungen dieses DPA und den DPF-GRUNDSÄTZEN EU-U.S. und/oder den Swiss-U.S. DPF-Grundsätze, die Grundsätze gelten. Um mehr über das Data Privacy Framework (DPF)-Programm zu erfahren und unsere Zertifizierung einzusehen, besuchen Sie bitte https://www.dataprivacyframework.gov/. Die Liste der teilnehmenden Organisationen des Datenschutzrahmens (DPF) ist unter https://www.dataprivacyframework.gov/s/participant-search verfügbar. Unter bestimmten Bedingungen können Sie das entsprechende verbindliche Schiedsverfahren aufrufen. Die Federal Trade Commission ist zuständig für die Einhaltung des EU-U.S. Data Privacy Framework (EU-U.S. DPF) durch Alaio, Inc. und die britische Erweiterung des EU-U.S. DPF sowie des Swiss-U.S. Datenschutzrahmenwerk (Swiss-U.S. DPF).

11.3.3 Beilegung von Streitigkeiten

Interner Beschwerdemechanismus von Alaio, Inc. In Übereinstimmung mit dem EU-U.S. DPF, der britischen Erweiterung des EU-U.S. DPF und dem Swiss-U.S. DPF, Alaio, Inc verpflichtet sich, Beschwerden im Zusammenhang mit den DPF-Grundsätzen über unsere Erfassung und Verwendung Ihrer personenbezogenen Daten zu lösen. Personen aus der EU, dem Vereinigten Königreich und der Schweiz mit Anfragen oder Beschwerden bezüglich unseres Umgangs mit personenbezogenen Daten, die wir im Vertrauen auf das EU-U.S.

DPF, die britische Erweiterung des EU-U.SDPF und des Swiss-U.S. DPF sollten sich zunächst an Alaio, Inc unter privacy@bitrix24.com wenden.

Alternative Streitbeilegungsstelle

In Einhaltung des EU-U.S. DPF, der UK Extension to the EU-U.S. DPF und des Swiss-U.S. DPF, Alaio, Inc verpflichtet sich, ungelöste Beschwerden über unseren Umgang mit personenbezogenen Daten, die wir im Vertrauen auf das EU-U.S. DPF, die UK-Erweiterung erhalten, an das EU-U.S. DPF und das Swiss-U.S. DPF an JAMS, einen Anbieter alternativer Streitbeilegung mit Sitz in den Vereinigten Staaten. Wenn Sie von uns keine rechtzeitige Bestätigung Ihrer Beschwerde im Zusammenhang mit den DPF-Grundsätzen erhalten oder wenn wir Ihre Beschwerde im Zusammenhang mit den DPF-Grundsätzen nicht zu Ihrer Zufriedenheit bearbeitet haben, besuchen Sie bitte https://www.jamsadr.com/ für weitere Informationen oder um eine Beschwerde einzureichen. Die Dienste von JAMS werden Ihnen kostenlos zur Verfügung gestellt.

11.4 Die Sicherheit von Daten und Rechten betroffener Personen gemäß der DSGVO bei den Datenverarbeitungsvorgängen in der Russischen Föderation wird durch die angemessenen Garantien nach Artikel 46 der DSGVO, insbesondere die von der Europäischen Kommission im Einklang mit dem Prüfverfahren angenommenen Standardklauseln gewährleistet. Die Europäische Kommission hat bestimmt, dass die Standardklauseln hinreichende Garantien für den Datenschutz bei grenzübergreifend zu übermittelten Daten bieten. Sie sind berechtigt, Informationen über diese vertraglichen Garantien zu erhalten (kontaktieren Sie dazu bitte unseren Datenschutzbeauftragten).

12 ANWENDBARES RECHT

12.1. Dieser AVV (einschließlich sämtlicher außervertraglichen Sachverhalte und Verpflichtungen, die sich daraus ergeben oder im Zusammenhang damit stehen) unterliegt den gesetzlichen Vorschriften der Republik Zypern und ist in Übereinstimmung damit auszulegen.

12.2 Für alle Streitigkeiten, Widersprüche, Gerichtsverfahren und Ansprüche zwischen den Parteien im Zusammenhang mit diesem Vertrag (einschließlich sämtlicher außervertraglichen Sachverhalte und Verpflichtungen, die sich daraus ergeben oder im Zusammenhang damit stehen) sind die zypriotischen Gerichte zuständig.

12.3 Für die im Punkt 11.3 angeführten Datenübermittlungen in die Länder außerhalb des EWR, die durch die Verantwortlichen in der EU an die Auftragsverarbeiter außerhalb der EU vorgenommen werden und die durch angemessene Garantien gemäß Artikel 46 der DSGVO, speziell durch die von der Europäischen Kommission im Einklang mit dem Prüfverfahren angenommenen Standarddatenschutzklauseln geschützt sind, sowie für Kunden, sofern die Verarbeitung im Rahmen der Tätigkeit einer Niederlassung in einem anderen Land des EWR als der Republik Zypern erfolgt, und/oder Kunden, welche Leistungen an betroffene Personen in einem anderen Land des EWR als der Republik Zypern erbringen, gilt die

Aufsichtsbehörde in der Republik Zypern als die federführende Aufsichtsbehörde gemäß Artikel 56 der DSGVO.

Die Aufsichtsbehörde der einzigen Niederlassung von Alaio im EWR, die zuständig ist, als federführende Aufsichtsbehörde für grenzüberschreitende Verarbeitung durch den Auftragsverarbeiter in Übereinstimmung mit dem in Artikel 60 der DSGVO festgelegten Verfahren aufzutreten, ist die Aufsichtsbehörde in der Republik Zypern.

13 ÄNDERUNGEN DIESES AVV

13.1 Alaio ist berechtigt, Änderungen an diesem AVV vorzunehmen, wenn diese Änderung:

(a) durch diesen AVV ausdrücklich gestattet ist;

(b) die Änderung der Firma oder der Rechtsform der juristischen Person betrifft;

(c) notwendig ist, um die geltenden gesetzlichen Bestimmungen, Vorschriften, einen gerichtlichen Beschluss oder eine von einer Regulierungs- oder Regierungsbehörde erlassene Richtlinie einzuhalten, oder

(d) wenn diese Änderung: (i) zu keiner Verschlechterung der allgemeinen Sicherheit der Services des Auftragsverarbeiters führt; (ii) zu keiner Erweiterung des Umfangs beziehungswiese Beseitigung der Beschränkungen für die Verarbeitung personenbezogener Daten führt und (iii) nach vernünftiger Auffassung von Bitrix24 keine sonstigen erheblichen negativen Auswirkungen auf die Rechte des Kunden aus diesem AVV hat.

13.2 Benachrichtigung über die Änderungen. Sollte Alaio beabsichtigen, diesen AVV zu ändern, wird Alaio spätestens 30 Tage (bzw. einen entsprechend kürzeren Zeitraum, der kraft geltender gesetzlicher Bestimmungen, Vorschriften, eines gerichtlichen Beschlusses oder einer von einer Regulierungs- oder Regierungsbehörde erlassenen Richtlinie notwendig ist) vor dem Inkrafttreten der Änderung den Administrator darüber in Kenntnis setzen, indem Alaio entweder: (a) eine E-Mail an die E-Mail-Adresse für Benachrichtigungen versendet oder (b) den Administrator über die Benutzeroberfläche der Services des Auftragsverarbeiters darauf hinweist. Widerspricht der Administrator einer solchen Änderung, ist der Administrator berechtigt, den Vertrag durch eine schriftliche Erklärung gegenüber Alaio zu kündigen, die spätestens 30 Tage nachdem Alaio ihn über die Änderung benachrichtigt zu erfolgen hat.

Anhang 1

GEGENSTAND UND EINZELHEITEN ZUM GEGENSTAND DER DATENVERARBEITUNG

Betroffene Personen. Die übermittelten personenbezogenen Daten umfassen folgende Kategorien betroffener Personen:

1. Betroffene Personen, über die Alaio im Rahmen der Bereitstellung von Services des Auftragsverarbeiters personenbezogene Daten erhebt, und/oder

2. Betroffene Personen, deren personenbezogene Daten im Rahmen der Bereitstellung von Services des Auftragsverarbeiters von dem Administrator, auf dessen Anweisung oder in dessen Auftrag an Alaio übermittelt werden.

Sie umfassen:

- Mitarbeiter, einschließlich ehrenamtlicher Mitarbeiter, Vertreter, Zeitarbeitnehmer und Aushilfskräfte
- Nutzer und Kunden (einschließlich deren Mitarbeiter)
- Lieferanten (einschließlich deren Mitarbeiter)
- Gesellschafter oder Träger
- Antragsteller, Korrespondenzpartner und Frageteller
- Berater, Gutachter und sonstige Sachverständige

Datenkategorien. Die übermittelten personenbezogenen Daten betreffen folgende Datenkategorien:

- persönliche Daten, einschließlich Informationen, welche die betroffene Person und ihre persönlichen Merkmale kennzeichnen, unter anderem Vor- und Nachname und die geschäftlichen Kontaktinformationen;
- Kommunikationsmetadaten;
- Mitarbeiterdaten, unter anderem gegebenenfalls die Arbeitszeit und der Standort (vorbehaltlich der Nutzerzustimmung im Rahmen der Zeiterfassung);
- bereitgestellte Waren und Dienstleistungen und die damit zusammenhängenden Informationen, einschließlich der Angaben zu bereitgestellten Waren und Dienstleistungen, ausgestellten Lizenzen sowie Verträgen;
- Angaben zu dem Land, der Stadt, dem Bundesstaat und der Region;
- Online-Identifizierungsmerkmale;
- Gerätekennungen;´
- Strukturierte Dokumentationsdaten
- persönliche Bilder, Audio- und Videoaufnahmen;

- Angaben zu Lebensgewohnheiten und sozialen Verhältnissen;
- Unterschriften.

Besondere Datenkategorien (falls zutreffend):

Nicht verfügbar

Verarbeitungsvorgänge. Auf die personenbezogenen Daten finden folgende grundlegende Verarbeitungsvorgänge Anwendung (bitte auflisten):

- IT, digitale, technische oder Telekommunikationsleistungen, unter anderem Bereitstellung von Technologieprodukten und Dienstleistungen, Telekommunikations- und Netzwerkdiensten, digitalen Dienstleistungen, Hosting, Cloud- und
  Kundendienstleistungen und Softwarelizenzierung. Dies umfasst unter anderem:

- das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, das Abfragen, die Verwendung, die Offenlegung, das Löschen oder die Vernichtung personenbezogener Daten des Kunden zum Zwecke der Bereitstellung von Services und der damit verbundenen technischen Unterstützung an den Kunden in Übereinstimmung mit diesem Auftragsverarbeitungsvertrag. Zu den Services zählen: Social Intranet, Projektmanagement und Aufgaben, Chat und Video, Dokumentenmanagement und Bitrix24.Drive, Kalender, E-Mail, CRM, Websites, Kommunikationskanäle, Contact Center, Telefonie, Zeitmanagement, CRM-Marketing, Workflows, eCommerce, On-Premise Version.

Anhang 2

SICHERHEITSMASSNAHMEN

Alaio verpflichtet sich, die in diesem Anhang 2 festgelegten Sicherheitsmaßnahmen umzusetzen und aufrechtzuerhalten. Alaio ist berechtigt, die Sicherheitsmaßnahmen von Zeit zu Zeit zu verbessern oder zu ändern, vorausgesetzt, dass solche Verbesserungen und Änderungen zu keiner Verschlechterung der allgemeinen Sicherheit der Services des Auftragsverarbeiters führen.

1. WICHTIGSTE DATENSCHUTZGRUNDSÄTZE BEI BITRIX24

1.1 Alle IT-Systeme von Alaio sind gegen einen unbefugten Zugang geschützt.

1.2 Alle IT-Systeme von Alaio werden ausschließlich in Übereinstimmung mit den maßgeblichen Unternehmensrichtlinien verwendet.

1.3 Alle Mitarbeiter von Alaio und alle Dritten, die befugt sind, die IT-Systeme zu nutzen, einschließlich unter anderem Unterauftragsverarbeitern, haben sicherzustellen, dass sie mit diesen Richtlinien vertraut sind und diese zu jedem Zeitpunkt befolgen.

1.4 Alle direkten Vorgesetzen haben sicherzustellen, dass alle unterstellten und weisungsgebundenen Mitarbeiter und Unterauftragsverarbeiter diese Richtlinien gemäß Absatz 2.3. stets befolgen und einhalten.

1.5 Alle auf den IT-Systemen gespeicherten Daten werden sicher und im Einklang mit den maßgeblichen Bestandteilen der EU-Datenschutzverordnung 2016/679 („DSGVO“) und allen anderen derzeit geltenden und in Zukunft zu verabschiedenden Datenschutzvorschriften verwaltet.

1.6 Allen auf den IT-Systemen gespeicherten Daten werden entsprechend ihrer Vertraulichkeitsstufe eingeordnet. Alle einer Vertraulichkeitsstufe eingeordneten Daten werden entsprechend ihrer Klassifizierung behandelt.

1.7 Alle auf den IT-Systemen gespeicherten Daten stehen ausschließlich denjenigen Nutzern zur Verfügung, die den Zugang zu ihnen aus legitimen Gründen benötigen.

1.8 Alle auf den IT-Systemen gespeicherten Daten sind gegen einen unbefugten Zugang und gegen eine unrechtmäßige Verarbeitung geschützt.

1.9 Alle auf den IT-Systemen gespeicherten Daten sind gegen den Datenverlust und die Datenbeschädigung geschützt.

1.10 Alle Verletzungen des Schutzes personenbezogener Daten auf den IT-Systemen oder von den darauf gespeicherten Daten werden gemeldet und anschließend von der IT-Abteilung untersucht.

2. SICHERHEITSMASSNAHMEN BEI SOFTWARE

2.1 Sämtliche auf den IT-Systemen verwendeten Softwareanwendungen (einschließlich unter anderem Betriebssystemen, einzelner Softwareanwendungen und Firmware) werden auf dem neuesten Stand gehalten und alle entsprechenden Software-Aktualisierungen, -Korrekturen, -Nachbesserungen und dazwischenliegende Produktaktualisierungen werden durchgeführt.

2.2 Beim Feststellen von Sicherheitslücken bei der Software werden diese Sicherheitslücken sofort geschlossen. Andernfalls wird die Software aus den IT-Systemen entfernt, bis die Sicherheitslücke erfolgreich geschlossen werden kann.

2.3 Die Mitarbeiter von Alaio dürfen nur mit einer Genehmigung des IT-Managers eigene Software installieren. Dies gilt unabhängig davon, ob diese Software auf einem physischen Datenträger zur Verfügung steht oder heruntergeladen wurde. Alle Softwareanwendungen müssen von dem IT-Manager genehmigt werden und dürfen nur dann installiert werden, wenn die Installation kein Sicherheitsrisiko für die IT-Systeme darstellt und wenn sie gegen keine auf diese Software gegebenenfalls anwendbaren Lizenzverträge verstoßt.

3. ANTIVIREN-SICHERHEITSMASSNAHMEN

3.1 Die IT-Systeme von Alaio (einschließlich aller Computer und Server) sind durch die geeigneten Antiviren-, Firewall- und sonstige geeignete Internet-Sicherheitssoftware geschützt. Auf allen Softwareanwendungen wurden die neuesten Aktualisierungen und Sicherheitsdefinitionen installiert.

3.2 Alle IT-Systeme von Alaio sind durch die Antivirensoftware geschützt und durchlaufen mindestens einmal pro Woche eine vollständige Systemprüfung.

3.3 Alle physischen Speichermedien (z.B. USB-Speichersticks oder alle Arten von Datenträgern), die von den Mitarbeitern für die Dateienübermittlungen verwendet werden, werden vor der Übermittlung auf Viren überprüft. Solche Viren-Prüfungen werden von dem Leiter der IT-Abteilung durchgeführt.

3.4 Die Mitarbeiter von Alaio dürfen nur mit Genehmigung des IT-Managers die Dateien über Cloud-Speichersysteme übermitteln. Alle von einem Cloud-Speicher heruntergeladenen Dateien werden beim Herunterladen auf Viren geprüft.

3.5 Alle an Dritte außerhalb des Unternehmens zu übermittelten Dateien, unabhängig davon, ob sie per E-Mail, auf physischen Datenträgern oder auf andere Weise (z.B. über einen gemeinsamen Cloud-Speicher) bereitgestellt werden, werden vor der Übermittlung im Rahmen des Übermittlungsprozesses auf Viren untersucht.

4. **SICHERHEITSMASSNAHMEN BEI HARDWARE**

4.1 IT-Systeme von Alaio befinden sich in sicher verschlossenen Räumen (die von befugten Nutzern mit einer Smartcard betreten werden können).

4.2 Alle IT-Systeme, die für die gewöhnliche Nutzung durch die Nutzer nicht vorgesehen sind (einschließlich unter anderem der Server, Netzwerkausstattung und Netzwerkinfrastruktur) befinden sich in abgesicherten klimatisierten Räumen in verschlossenen Schränken, zu denen ausschließlich bestimmte Mitarbeiter der IT-Abteilung Zugang haben).

4.3 Alle von dem Unternehmen bereitgestellten mobilen Geräte (einschließlich unter anderem Laptops, Tablets und Smartphones) werden stets sicher befördert und sorgfältig behandelt.

5. **ZUGRIFFSSICHERHEIT**

5.1. Die Zugriffsrechte auf alle IT-Systeme werden auf Grundlage der Zuständigkeitsebenen der Mitarbeiter innerhalb der Unternehmensstruktur von Alaio und der Notwendigkeit für die Ausübung ihrer beruflichen Funktionen festgelegt. Die Mitarbeiter erhalten keinen Zugriff auf die IT-Systeme oder elektronische Daten, die begründeterweise zur Ausübung ihrer beruflichen Funktionen nicht erforderlich sind.

5.2 Alle IT-Systeme (und insbesondere mobile Geräte, darunter unter anderem Laptops, Tablets und Smartphones) werden durch ein sicheres Passwort oder den sicheren Zugangscode beziehungsweise durch andere sichere Anmeldeverfahren geschützt, die von der IT-Abteilung für geeignet erklärt und genehmigt wurden.

5.3 Auf alle Passwörter finden folgende Sicherheitsmaßnahmen Anwendung:

a) Die Passwörter müssen aus mindestens 8 Zeichen bestehen;

b) Sie müssen eine Kombination aus Groß- und Kleinbuchstaben, Nummern und Symbolen enthalten;

c) Sie müssen mindestens einmal jede 90 Tage geändert werden;

d) Sie dürfen mit den vorherigen Passwörtern gleich sein;

e) Sie dürfen nicht offensichtlich oder leicht zu erraten (z.B. Geburtstage oder andere bedeutungsvolle Daten, Namen, Ereignisse oder Orte, u.s.w.) sein und

f) Sie müssen von den einzelnen Nutzern selbst erstellt worden sein.

5.4 Alle IT-Systeme mit Bildschirmen und Benutzerinterface-Geräten (z.B. Maus, Tastatur, Touchscreen usw.) werden durch einen mit Passwort geschützten Bildschirmschoner geschützt, der sich nach 5 Minuten der Inaktivität aktiviert.

6. **SICHERHEIT BEI DATENSPEICHERUNG**

1.1 Alle Daten und insbesondere personenbezogenen Daten werden durch die Verwendung von Passwörtern und der OTP-Autorisierung sicher gespeichert.

1.2 Auf den mobilen Geräten (einschließlich unter andrem Laptops, Tablets und Smartphones) werden keine personenbezogenen Daten aufbewahrt. Dies gilt unabhängig davon, ob es sich bei dem Gerät um ein Gerät von Bitrix24 handelt oder nicht.

1.3 Keine Daten und insbesondere keine personenbezogenen Daten werden auf einen persönlichen Computer oder ein persönliches Gerät des Mitarbeiters übertragen, es sei denn, dass es sich bei dem betreffenden Mitarbeiter um einen im Auftrag von Alaio tätigen Unterauftragsverarbeiter handelt und sich dieser Unterauftragsverarbeiter verpflichtet hat, die Datenschutzrichtlinie des Unternehmens und die DSGVO vollumfänglich einzuhalten.

7. **DATENSCHUTZ**

7.1 Alle von Alaio erhobenen, gespeicherten und verarbeiteten personenbezogenen Daten (gemäß der DSGVO-Definition) werden streng nach Maßgabe der in der DSGVO festgelegten Grundsätze und Bestimmungen sowie der Datenschutzrichtlinie des Unternehmens erhoben, gespeichert und verarbeitet.

7.2 Alle Nutzer, die für und im Auftrag von Alaio Daten verarbeiten, unterliegen stets den Bestimmungen der Datenschutzrichtlinie des Unternehmens und haben diese einzuhalten. Insbesondere gilt Folgendes:

a) Alle E-Mails, die vertrauliche oder sensible personenbezogene Daten enthalten, werden durch die Verwendung des TLS SSL-Protokolls verschlüsselt;

b) Alle E-Mails, die vertrauliche oder sensible personenbezogene Daten enthalten, werden als „vertraulich“ gekennzeichnet;

c) Vertrauliche und sensible personenbezogene Daten dürfen ausschließlich über gesicherte Netzwerke übermittelt werden; Übermittlungen über ungesicherte Netzwerke sind unter keinen Umständen zulässig;

d) Alle physisch zu übermittelnden vertraulichen und sensiblen personenbezogenen Daten, einschließlich der Übermittlung auf elektronischen Speichermedien, werden in geeigneten Behältern, die mit als „vertraulich” beschriftet sind, transportiert.

e) Werdenvertrauliche oder sensible personenbezogene Daten auf einem Computerbildschirm angezeigt und wird der betreffende Computer für einen Zeitraum unbeaufsichtigt gelassen, sind die Mitarbeiter verpflichtet, den Computer und den Bildschirm vor dem Verlassen zu sperren.

7.3 Alle Anfragen bezüglich des Datenschutzes sind an die Datenschutzbeauftragte, Frau Elena Riazanova (info@quick-gdpr.co.uk), zu richten.

8. RECHENZENTREN & NETZWERKSICHERHEIT DES HOSTING-ANBIETERS

Alaio nutzt die Amazon Web Services zur Speicherung und Analyse von Daten, einschließlich der AWS Cloud Infrastruktur in der Region Europa (Frankfurt) und der Region Europa (Irland).

VERFÜGBARKEIT

AWS kennt alle kritischen Systemkomponenten, die erforderlich sind, um die Verfügbarkeit unseres Systems zu erhalten und den Betrieb im Fall eines Ausfalls wieder aufzunehmen. Kritische Systemkomponenten werden an mehreren, voneinander isolierten Standorten (Availability Zones genannt) gesichert. Jede Availability Zone ist auf einen unabhängigen Betrieb mit hoher Zuverlässigkeit ausgelegt. Die Availability Zones sind vernetzt. Dies ermöglicht Ihnen die Nutzung von Anwendungen, für die ein automatischer, unterbrechungsfreier Failover zwischen den Availability Zones eingerichtet ist. Extrem ausfallsichere Systeme und eine daraus resultierende Serviceverfügbarkeit sind Bestandteil des Systemdesigns. AWS-Kunden profitieren durch den Einsatz von Availability Zones und Datenreplikation von extrem kurzen Wiederherstellungszeiträumen und Wiederherstellungspunktzielen sowie höchstmöglicher Serviceverfügbarkeit.

PLAN ZUR AUFRECHTERHALTUNG DES BETRIEBS:

Der AWS-Betriebskontinuitätsplan bestimmt Maßnahmen zur Vermeidung und Verringerung von Störungen durch Umwelteinflüsse. Er enthält betriebliche Details zu den Maßnahmen, die vor, während und nach einem entsprechenden Ereignis ergriffen werden. Der Betriebskontinuitätsplan wird durch Tests gestützt, die auch Simulationen verschiedener Szenarios umfassen. Während und nach diesen Tests dokumentiert AWS die Leistung seiner Mitarbeiter und Prozesse, Korrekturmaßnahmen und die abgeleiteten Erfahrungen zur kontinuierlichen Verbesserung.

DATENTRÄGERVERNICHTUNG

Medienspeichergeräte, auf denen Kundendaten gespeichert sind, werden von AWS als kritisch eingestuft und deshalb über ihren gesamten Lebenszyklus entsprechend als höchst dringlich behandelt. AWS hat bestehende Normen, wie die Geräte installiert, betrieben und irgendwann zerstört werden, wenn sie nicht mehr verwendet werden. Wenn ein Speichergerät das Ende seines Lebenszyklus erreicht hat, wird es gemäß den in NIST 800-88 beschriebenen Techniken stillgelegt. Medien, auf denen Kundendaten gespeichert wurden, werden erst nach erfolgter Stilllegung aus der Hand von AWS gegeben.

INFRASTRUKTURWARTUNG

Gerätewartung. AWS überwacht und wartet die elektrischen und mechanischen Geräte präventiv, um den unterbrechungsfreien Betrieb der Systeme in den AWS-Rechenzentren zu gewährleisten. Die Gerätewartung wird von qualifiziertem Personal entsprechend einem dokumentierten Wartungszeitplan durchgeführt.

Umweltmanagement. AWS überwacht elektrische und mechanische Systeme und Anlagen, sodass Probleme sofort erkannt werden. Hierfür werden fortlaufend Audit-Tools und Informationen der Gebäudemanagement- und elektrischen Überwachungssysteme ausgewertet. Es werden vorbeugende Wartungen vorgenommen, um eine kontinuierliche Funktionsfähigkeit der Anlagen sicherzustellen.

GOVERNANCE UND RISIKO

Risikomanagement für Rechenzentren. Das AWS Security Operations Center führt regelmäßig Bedrohungs- und Schwachstellenprüfungen der Rechenzentren durch. Die fortlaufende Bewertung und Abwehr von potenziellen Schwachstellen erfolgt über die Risikobewertungsaktivitäten der Rechenzentren. Diese Bewertung wird zusätzlich zum Risikobewertungsprozess auf Unternehmensebene durchgeführt, um Risiken für das Unternehmen als Ganzes zu erkennen und zu verwalten. Dabei werden auch regionale behördliche und Umweltrisiken berücksichtigt.

Sicherheitsbescheinigungen von Dritten. Durch Prüfungen der AWS-Rechenzentren durch Dritte, wie in unseren Drittanbieterberichten dokumentiert, stellt AWS sicher, dass angemessene Sicherheitsmaßnahmen implementiert wurden, die zum Erwerb von Sicherheitszertifikaten erforderlich sind. Abhängig vom Compliance-Programm und dessen Anforderungen können externe Prüfer die Entsorgung von Medien testen, die Aufzeichnungen der Sicherheitskameras prüfen, die Eingänge und Korridore eines Rechenzentrums beobachten, die elektronischen Zugangskontrollgeräte testen und die Anlagen des Rechenzentrums untersuchen.

Netzwerke und Übertragungen.

Datenübertragung. Die Rechenzentren von Alaio sind über private Verbindungen, die durch AWS-Netzwerk-Firewalls geschützt werden vernetzt und ermöglichen sichere Datenübertragungen. Dadurch werden die Vertraulichkeit, Integrität und Verfügbarkeit von Netzwerken geschützt und die Daten können während einer elektronischen Übermittlung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

Reaktion auf Verletzungen des Schutzes personenbezogener Daten. Alaio überwacht eine Vielzahl an Kommunikationswegen auf Verletzungen des Schutzes personenbezogener Daten. Das Sicherheitspersonal von Alaio reagiert unverzüglich auf die bekannt gewordenen Verletzungen.

Externe Angriffsoberfläche. Alaio analysiert potentielle Angriffsvektoren und setzt bei den nach außen gerichteten Systemen geeignete herstellereigene Technologien ein, die dafür speziell entwickelt wurden.

Verschlüsselungstechnologien. Alaio verwendet eine HTTPS-Verschlüsselung (auch bekannt als SSL bzw. TLS Verbindung).

9. SICHERHEIT BEI UNTERAUFTRAGSVERARBEITERN

Vor einer Beauftragung von Unterauftragsverarbeitern überprüft Alaio die Sicherheit und Datenschutzpraktiken der Unterauftragsverarbeiter. Dadurch wird sichergestellt, dass Unterauftragsverarbeiter über die Sicherheits- und Datenschutzstandards verfügen, die für ihren Zugang zu den Daten und für die von ihnen bereitzustellenden Services angemessen sind. Nach der Bewertung der von einem Unterauftragsverarbeiter ausgehenden Risiken durch Alaio und stets vorbehaltlich der Einhaltung der im Abschnitt 7 festgelegten Anforderungen wird der Unterauftragsverarbeiter aufgefordert, die entsprechenden Sicherheits-, Vertraulichkeits- und Geheimhaltungsvereinbarungen abzuschließen.