

Vertrag über die Auftragsverarbeitung personenbezogener Daten

zwischen

Agentur Z GmbH, Zielstrasse 185, 8106 Adlikon,
- als Verantwortlicher (nachfolgend Auftraggeber) -

und der

alixon gmbh, Aarepark 2a, 5000 Aarau, Schweiz
- als Auftragsbearbeiter (nachfolgend Auftragnehmer) -

Präambel

Der Auftraggeber und der Auftragnehmer haben eine Vereinbarung abgeschlossen (nachfolgend **Hauptvertrag**), in deren Rahmen der Auftragnehmer für den Auftraggeber Arbeiten oder Dienstleistungen oder gegebenenfalls sonstige Leistungen, wie im Hauptvertrag festgelegt, erbringt. Der Hauptvertrag wurde in den meisten Fällen informell durch Angebot und Bestellung geschlossen.

Zum Zwecke der Erfüllung des Hauptvertrags erhält der Auftragnehmer unter Umständen Zugang zu personenbezogenen Daten, die dem Auftragnehmer durch den Auftraggeber direkt oder in dessen Auftrag durch Dritte offengelegt oder auf andere Weise zur Verfügung gestellt werden (nachfolgend **personenbezogene Daten**).

Die Parteien möchten sicherstellen, dass die durch den Auftragnehmer im Auftrag des Auftraggebers direkt oder durch Dritte durchgeführte Verarbeitung personenbezogener Daten im Rahmen des Hauptvertrags den geltenden Datenschutzgesetzen entspricht, und sich dabei auf bestimmte Bedingungen für die genannte Datenverarbeitung verständigen, die in diesem Nachtrag zum Datenschutz (Auftraggeber - Auftragnehmer) (im Folgenden der **Vertrag**) festgelegt sind.

1. Begriffsdefinitionen

1.1. Geltende Datenschutzgesetze

Geltende Datenschutzgesetze meint das neue Schweizer Bundesgesetz über den Datenschutz (nDSG), die neue Schweizer Verordnung zum Bundesgesetz über den Datenschutz.

1.2. Verantwortlicher

Verantwortlicher ist die natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 5 lit. j nDSG).

1.3. Auftragsbearbeiter

Auftragsbearbeiter ist die natürliche oder juristische Person, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 5 lit. k nDSG).

1.4. Personenbezogene Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen (nachfolgend betroffene Person); als bestimmbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels 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, identifiziert werden kann (Art. 5 lit. a nDSG).

1.5. Bearbeitung

Bearbeitung ist jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten (Art. 5 lit. d nDSG).

1.6. Bekanntgeben

Bekanntgeben ist das Übermitteln oder Zugänglichmachen von Personendaten (Art. 5 lit. e nDSG).

2. Angaben zur Datenverarbeitung

2.1. Hosting

Der Auftragnehmer stellt ein Internet-Hosting für den Verantwortlichen zur Verfügung. Dieses kann Website, E-Mail Server sowie DNS umfassen.

2.2. verein-web: adhocVoices.ch

Verwaltung der Mitglieder und weiterer Personen im Umfeld des Vereins. Erfasst werden Name und Adresse sowie weitere relevante Informationen, welche für den Betrieb des Vereins benötigt werden.

Auf der Internetplattform kann der Verantwortliche Benutzer anlegen, und diesen Rechte für den Zugriff auf die Daten erteilen. Dazu werden die Login Daten gespeichert. Die erteilten Rechte liegen in der Verantwortung des Verantwortlichen.

3. Dauer des Auftrags

Die Dauer der Auftragsverarbeitung ist unbefristet und kann ordentlich oder ausserordentlich gekündigt werden.

4. Pflichten des Auftragnehmers

4.1. Weisungsgemässe Verarbeitung

Der Auftragnehmer verpflichtet sich, die Daten ausschliesslich für die Zwecke des Hauptvertrags einschliesslich dieses Vertrags sowie gemäss den dokumentierten Instruktionen/Weisungen des Auftraggebers zu verarbeiten. Dies gilt insbesondere auch bezüglich der Übermittlung der Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union, der Mitgliedstaaten oder eines Nicht-EU-Mitgliedstaats, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

Der Auftraggeber kann jederzeit neue Instruktionen erlassen, ergänzen oder bestehende Instruktionen ändern. Dies umfasst auch Instruktionen im Hinblick auf die Berichtigung, Löschung und Sperrung personenbezogener Daten. Alle erteilten Instruktionen sind sowohl vom Auftraggeber als auch vom Auftragnehmer schriftlich zu dokumentieren.

Ist der Auftragnehmer der Ansicht, dass eine Instruktion des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstösst, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Instruktion ablehnen.

Im Übrigen bleiben die Pflichten, die dem Auftragnehmer direkt aus den anwendbaren Datenschutzgesetzen entstehen, wie beispielsweise die Erstellung eines Verzeichnisses der vorliegenden Auftragsverarbeitung gemäss Art. 12 nDSG, erhalten und von diesem Vertrag unberührt.

4.2. Pflicht zur Verschwiegenheit

Der Auftragnehmer verpflichtet sich und leistet Gewähr dafür, dass er alle mit der Datenverarbeitung betrauten Personen, einschliesslich Erfüllungsgehilfen, vor Aufnahme der Tätigkeit zur Vertraulichkeit in schriftlicher Form verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen, und dass die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung betrauten Personen auch nach Beendigung ihrer Tätigkeit beim Auftragnehmer bestehen bleibt. Der Auftragnehmer haftet für ein etwaiges Zuwiderhandeln der mit der Datenverarbeitung betrauten Personen, einschliesslich Erfüllungsgehilfen, wie für sein eigenes Verhalten.

4.3. Schutzmassnahmen des Auftragnehmers

Der Auftragnehmer verpflichtet sich und leistet Gewähr dafür, dass er alle erforderlichen Massnahmen zur Gewährleistung der Sicherheit der Bearbeitung gemäss Art. 7 und 8 nDSG ergriffen hat und aufrechterhält, um eine unbefugte Verarbeitung, einen Verlust oder eine Beschädigung personenbezogener Daten zu verhindern. Dies beinhaltet insbesondere die Mindestvorkehrungen, welche in Anhang B beschrieben sind.

4.4. Unterstützungspflichten

Der Auftragnehmer ist verpflichtet, den Auftraggeber auf Verlangen bei der Einhaltung der geltenden Datenschutzgesetze jederzeit und soweit möglich zu unterstützen.

a. Anträge und Rechte betroffener Personen

Der Auftragnehmer verpflichtet sich, den Auftraggeber mit geeigneten technischen und organisatorischen Massnahmen zu unterstützen, damit der Auftraggeber seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Personen (insbesondere Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit nachkommen kann, und überlässt dem Auftraggeber alle dafür notwendigen und ihm zur Verfügung stehenden Informationen.

Wird ein entsprechender Antrag an den Auftragnehmer gerichtet, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten. Der Auftragnehmer muss die Beantwortung solcher Anträge dem Auftraggeber überlassen, es sei denn, er ist gesetzlich dazu verpflichtet. In jedem Fall vereinbaren die Parteien, die Beantwortung solcher Anträge gegenseitig abzusprechen.

b. Weitere Informations- und Unterstützungspflicht

Der Auftragnehmer verpflichtet sich, den Auftraggeber unter Berücksichtigung der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 7, 8, 22-24 nDSG genannten Pflichten zu unterstützen (Datensicherheitsmassnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgenabschätzung und vorherige Konsultation).

Der Auftragnehmer verpflichtet sich, den Auftraggeber unverzüglich zu benachrichtigen im Falle (i) eines etwaigen tatsächlichen oder mutmasslichen Datenschutzverstosses (dies gilt auch für Verstösse gegen den Hauptvertrag einschliesslich dieses Vertrags sowie etwaige sonstige Datenschutzverstösse gemäss nDSG) unter Angabe sämtlicher dem Auftragnehmer zur Verfügung stehenden Informationen gemäss Art. 24 Abs. 2 nDSG, (ii) etwaiger tatsächlicher oder drohender Beeinträchtigungen oder Mängel aufseiten des Auftragnehmers, die einer Einhaltung der Bestimmungen des Hauptvertrags einschliesslich dieses Vertrags entgegenstehen, (iii) des Vorliegens etwaiger Anträge auf Zugang sowie des tatsächlich erfolgten Zugangs zu personenbezogenen Daten durch Behörden, sofern diese Benachrichtigung nicht per Gesetz aus wichtigen Gründen des öffentlichen Interesses verboten ist.

4.5. Rückgabe oder Löschungspflicht bei Vertragsbeendigung

Der Auftragnehmer verpflichtet sich, nach Beendigung des Hauptvertrags einschliesslich dieses Vertrags oder auf Verlangen des Auftraggebers sämtliche personenbezogenen Daten, vorbehaltlich gesetzlicher Aufbewahrungspflichten, an den Auftraggeber nach seiner Wahl zurückzugeben oder zu löschen, ohne eine Kopie aufzubewahren, und die Löschung auf Anfrage gegenüber dem Auftraggeber entsprechend zu bestätigen.

4.6. Kontrollrechte des Auftraggebers

Der Auftragnehmer verpflichtet sich, dem Auftraggeber sämtliche Informationen zur Verfügung zu stellen, die erforderlich sind, um die Einhaltung dieses Vertrags durch den Auftragnehmer nachzuweisen und Überprüfungen, einschliesslich Inspektionen, durch den Auftraggeber selbst, einen vom Auftraggeber beauftragten Prüfer oder durch die Aufsichtsbehörde zu ermöglichen und aktiv zu unterstützen. Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen im Geschäftsbetrieb zu erfolgen.

5. Datensicherheit

Der Auftragnehmer hat angemessene technische und organisatorische Massnahmen zu ergreifen und aufrechtzuerhalten, so dass die Bearbeitung den Anforderungen der anwendbaren Datenschutzgesetze (insbesondere Art. 28 DSGVO) entspricht und den Schutz der Rechte der betroffenen Personen gewährleistet. Siehe Anhang B

6. Ort der Datenverarbeitung

Die Datenverarbeitungen werden nur an den Standorten durchgeführt, die im zugehörigen Hauptvertrag oder in diesem Vertrag in Anhang A vereinbart oder anderweitig vom Auftraggeber schriftlich genehmigt wurden.

7. Einsatz von Unterauftragsverarbeitern

Der Auftragnehmer ist nicht berechtigt, einen Unterauftragsverarbeiter heranzuziehen, ohne vorgängig die schriftliche Zustimmung des Auftraggebers einzuholen.

Beabsichtigte Änderungen des Unterauftragsverarbeiters sind dem Auftraggeber rechtzeitig schriftlich bekannt zu geben, sodass er diese gegebenenfalls untersagen kann. Der Auftragnehmer schliesst die erforderlichen schriftlichen Vereinbarungen zur Vertraulichkeit und zum Datenschutz mit dem Unterauftragsverarbeiter ab, welche mindestens so streng wie die Bestimmungen des Hauptvertrags einschliesslich dieses Vertrags sein müssen. Dabei hat der Auftragnehmer insbesondere sicherzustellen, dass der Unterauftragsverarbeiter dieselben Verpflichtungen eingetht und insbesondere auch die technischen und organisatorischen Massnahmen trifft, die dem Auftragnehmer aufgrund dieses Vertrags obliegen.

Der Auftragnehmer haftet gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Unterauftragsverarbeiters wie für sein eigenes Verhalten.

8. Ausführung zusätzlicher Vereinbarungen

Der Auftragnehmer stimmt zu, auf Verlangen des Auftraggebers im Rahmen der bestehenden Verträge weiterführende Vereinbarungen mit dem Auftraggeber zur Verarbeitung personenbezogener Daten abzuschliessen, sofern der Auftraggeber dies nach vernünftigem Ermessen für die Einhaltung des geltenden Datenschutzrechts als erforderlich erachtet.

9. Ausserordentliches Kündigungsrecht

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoss des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrags vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Dabei stellen insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 9 nDSG abgeleiteten Pflichten einen schweren Verstoss dar.

10. Bezug zu bestehenden Verträgen

- a. Die Anhänge zu diesem Vertrag bilden einen integrierenden Bestandteil des vorliegenden Vertrags.
- b. Steht eine in diesem Vertrag enthaltene Bestimmung im Widerspruch zum Hauptvertrag, gilt die im vorliegenden Vertrag enthaltene Bestimmung als massgeblich.
- c. Die Bestimmungen des vorliegenden Vertrags haben auch nach Beendigung des Hauptvertrags weiterhin Bestand, solange der Auftragnehmer im Besitz personenbezogener Daten des Auftraggebers ist.

11. Schlussbestimmungen

- a. Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- b. Sollten einzelne Bestimmungen dieses Vertrags ganz oder teilweise ungültig sein oder werden, so wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Die Parteien vereinbaren, die unwirksame Bestimmung durch eine wirksame Bestimmung zu ersetzen, welche dem wirtschaftlichen Sinn und Zweck der unwirksamen Bestimmung am nächsten kommt.
- c. Dieser Vertrag untersteht Schweizer Recht unter Ausschluss des Internationalen Privatrechts (IPRG). Ausschliesslicher Gerichtsstand für Streitigkeiten aus diesem Vertrag oder im Zusammenhang mit der Auslegung und Anwendung des vorliegenden Vertrags ist der Sitz des Auftragnehmers.

Unterschriften

Verantwortlicher

Adlikon, den 10.09.2023

Agentur Z GmbH, Susanne Dietze

Timestamp: 2023-09-10 12:02:28

IP Adresse: 84.75.50.201

Auftragnehmer

Aarau, den 10.09.2023

alixon gmbh
Aarepark 2a
CH-5000 Aarau
www.alixon.ch



Anhang A: Serverstandorte

A.1. Zürich, Schweiz: Nine Internet Solutions AG (Colo Zürich)

Zutrittskontrolle und Zugangskontrolle wird von Nine AG sichergestellt: Zertifiziert nach 27001

Der Auftragnehmer hat physischen Zugang zu den Servern über biometrischer Zugangskontrolle und physischem Schlüssel

Datenträgerkontrolle: Festplatten werden nach dem Einsatz mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt. Defekte Festplatten, die nicht sicher gelöscht werden können, werden mechanisch zerstört.

A.2. Aarau, Schweiz: Flying Supporter (Eniwa)

Zutrittskontrolle und Zugangskontrolle wird von Eniwa AG sichergestellt: Zertifiziert nach 27001.

Der Auftragnehmer hat physischen Zugang zu den Servern in Begleitung eines Mitarbeiters von Flying Supporter.

Datenträgerkontrolle: Festplatten werden nach dem Einsatz mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt. Defekte Festplatten, die nicht sicher gelöscht werden können, werden mechanisch zerstört.

Anhang B: Technische und organisatorische Massnahmen

Im Folgenden werden die auf Art. 7 und 8 nDSG und Art. 2 des Vorentwurfs der neuen Verordnung zum neuen Datenschutzgesetz basierenden technischen und organisatorischen Massnahmen beschrieben, die konkret vom Auftragnehmer im Zusammenhang mit der Verarbeitung personenbezogener Daten und der Erfüllung seiner Verpflichtungen gemäss dem Hauptvertrag einschliesslich diesem Vertrag als Mindestvorkehrungen zu ergreifen sind, um ein dem Risiko angemessenes Schutzniveau hinsichtlich des Datenschutzes und der Datensicherheit der überlassenen Daten zu gewährleisten

B.1. Vertraulichkeit

B.1.1. Zutrittskontrolle: Anforderung: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen

Der Auftragnehmer gewährleistet die Zutrittskontrolle zu seinen Räumlichkeiten durch geeignete Massnahmen.

Massnahmen: Siehe Anlage A: Serverstandorte

B.1.2. Zugangskontrolle: Anforderung: Schutz vor unbefugter Systembenutzung

Der Auftragnehmer gewährleistet die elektronische Zugangskontrolle durch geeignete Massnahmen:

- Siehe Anlage A: Serverstandorte

B.1.3. Zugriffskontrolle: Anforderung: kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

Der Auftragnehmer gewährleistet die Zugriffskontrolle durch geeignete Massnahmen:

- Standard-Berechtigungsprofile auf «Need-to-know-Basis», Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten.

B.1.4. Pseudonymisierung

Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt und gesondert aufbewahrt.

B.1.5. Fähigkeit der Systeme und Dienste

Der Auftragnehmer gewährleistet die Fähigkeit der Systeme und Dienste, wonach alle Funktionen des Systems und Dienste zur Verfügung stehen und auftretende Fehlfunktionen gemeldet und behoben werden.

B.2. Integrität

B.2.1. Weitergabekontrolle: Anforderung: kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

Der Auftragnehmer gewährleistet die Weitergabekontrolle durch geeignete Massnahmen:

- Alle Übertragungen finden nach dem Stand der Technik verschlüsselt statt.

B.2.2. Eingabekontrolle: Anforderung: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

Der Auftragnehmer gewährleistet die Eingabekontrolle durch geeignete Massnahmen:

- Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
- Änderungen der Daten werden protokolliert.

B.3. Verfügbarkeit und Belastbarkeit

B.3.1. Verfügbarkeitskontrolle: Anforderung: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust

Der Auftragnehmer gewährleistet die Verfügbarkeit sowie die rasche Wiederherstellbarkeit und das Löschen nach Gebrauch der Daten durch geeignete Massnahmen.

Backup- und Recovery-Konzept mit regelmässiger Sicherung aller relevanten Daten.

Bei den meisten Projekte steht ein Hot-Standby Server mit Datenreplikation in einem anderen Rechenzentrum bereit.

B.3.2. Trennungskontrolle: Anforderung: es muss gewährleistet sein, dass Daten, die für verschiedene Zwecke erhoben wurden, getrennt verarbeitet werden können

Der Auftragnehmer gewährleistet die getrennte Verarbeitung von Daten durch geeignete Massnahmen. Insbesondere müssen zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden.

B.4. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

B.4.1. Anforderung: regelmässige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Der Auftragnehmer führt jährlich eine Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung durch. Der resultierende Bericht wird auf Anfrage zur Verfügung gestellt.

B.4.2. Auftragskontrolle: Anforderung: keine Auftragsdatenverarbeitung im Sinne von Art. 9 nDSG ohne entsprechende Weisung des Auftraggebers

Der Auftragnehmer gewährleistet die Überprüfung der Unterauftragsverarbeiter durch geeignete Massnahmen.