Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO

Verantwortlicher (Auftraggeber):

Auftragsverarbeiter (Auftragnehmer):

openPetion gGmbH, Greifswalder Str. 4, 10405 Berlin
vertreten durch Geschäftsführer Jörg Mitzlaff

1. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes:

Vertrag über ein opTo Petitionstool vom ……

Der Auftragsverarbeiter verarbeitet dabei personenbezogene Daten für den Verantwortlichen im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Dauer des Auftrags

Der Vertrag beginnt am ..... und wird auf unbestimmte Zeit geschlossen. Die Kündigungsfrist ist 4 Wochen zum Jahresende.

Der Verantwortliche kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragsverarbeiter eine Weisung des Verantwortlichen nicht ausführen kann oder will oder der Auftragsverarbeiter Kontrollrechte des Verantwortlichen vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

Zwecke der Verarbeitung ist die Erbringung der vertraglich vereinbarten Leistung (sh. Ziff. II Vertrag vom 24.10.18/02.11.18)

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DS-GVO):

Es werden alle von Verarbeitungen im Sinne der DS-GVO vorgenommen.

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DS-GVO):

Alle Arten personenbezogener Daten, die openPetition im Auftrag verarbeitet, inklusive besonderer Kategorien personenbezogener Daten.

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO):

Mitarbeiter, Auftragsverarbeiter, Mitarbeiter des Auftragsverarbeiters, Besucher und Nutzer der Webseite des Auftragsverarbeiters.

3. Rechte und Pflichten sowie Weisungsbefugnisse des Verantwortlichen

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Verantwortliche verantwortlich. Gleichwohl ist der Auftragsverarbeiter verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Verantwortlichen gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Verantwortlichem und Auftragsverarbeiter abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Verantwortliche erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Der Verantwortliche ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Verantwortliche ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragsverarbeiters vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Verantwortlichen, Weisungsempfänger des Auftragsverarbeiters

Weisungsberechtigte Personen des Verantwortlichen sind:

(Vorname, Name, Organisationseinheit, Telefon)

Weisungsempfänger beim Auftragsverarbeiters sind:

Jörg Mitzlaff, Geschäftsführer, 030 234 750 39

(Vorname, Name, Organisationseinheit, Telefon)

Für Weisung zu nutzende Kommunikationskanäle:

openPetition gGmbH, Greifswalder Str. 4, 10405 Berlin /
joerg.mitzlaff@openpetition.de / 030 234 750 39

(genaue postalische Adresse/ E-Mail/ Telefonnummer)

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Verantwortlichen, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der

Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

Der Auftragsverarbeiter verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Verantwortlichen nicht erstellt.

Der Auftragsverarbeiter sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Verantwortlichen verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Die Datenträger, die vom Verantwortlichen stammen bzw. für den Verantwortlichen genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Der Auftragsverarbeiter hat über die gesamte Abwicklung der Dienstleistung für den Verantwortlichen insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:

Kontrolle hinsichtlich der Aktualität der TOM (siehe Anlage 1)

Das Ergebnis der Kontrollen ist zu dokumentieren.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Verantwortlichen, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Verantwortlichen hat der Auftragsverarbeiter im notwendigen Umfang mitzuwirken und den Verantwortlichen soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO). Er hat die dazu erforderlichen Angaben dem Verantwortlichen unverzüglich an folgende Stelle weiterzuleiten:

Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darauf aufmerksam machen, wenn eine vom Verantwortlichen erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Verantwortlichen nach Überprüfung bestätigt oder geändert wird.

Der Auftragsverarbeiter hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Verantwortliche dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragsverarbeiters dem nicht entgegenstehen.

Unabhängig davon hat der Auftragsverarbeiter personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Weisung des Verantwortlichen ein berechtigter Anspruch des Betroffenen aus Art. 16, 17 und 18 DS-GVO zugrunde liegt.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger Weisung oder Zustimmung durch den Verantwortlichen erteilen.

Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Verantwortliche - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Verantwortlichen beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO).

Der Verantwortliche kann die Einhaltung eines genehmigten Zertifizierungsverfahrens gem. Art. 42 DS-GVO durch den Auftragsverarbeiter als Faktor heranziehen, um die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen zu beurteilen.

Der Auftragsverarbeiter sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Hierzu wird bis auf weiteres folgendes vereinbart:

Der Auftragsverarbeiter ist berechtigt, für Inspektion eine angemessene Vergütung vom Verantwortlichen zu verlangen. Kontrollen jeder Art sind 14 Tage vorher anzumelden.

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragsverarbeiters) ist nur mit Zustimmung des Verantwortlichen gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen.

Der Auftragsverarbeiter bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind.

Der Auftragsverarbeiter verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Verantwortlichen die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragsverarbeiter sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz

2 lit. b und Art. 29 DS-GVO). Der Auftragsverarbeiter überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Ein betrieblicher Datenschutzbeauftragter ist beim Auftragsverarbeiter nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt. Die Verantwortliche Stelle für die datenschutzkonforme Verarbeitung von Daten nach Artikel 24 DSGVO ist bei openPetition der Geschäftsführende Gesellschafter Jörg Mitzlaff.

6. Mitteilungspflichten des Auftragsverarbeiters bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter teilt dem Verantwortlichen unverzüglich Störungen, Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Verantwortlichen nach Art. 33 und Art. 34 DS-GVO. Der Auftragsverarbeiter sichert zu, den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Verantwortlichen ist dem Auftragsverarbeiter nur mit Genehmigung des Verantwortlichen gestattet, Art. 28 Abs. 2 DS-GVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragsverarbeiter dem Verantwortlichen Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragsverarbeiter dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Verantwortlichen auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragsverarbeiter hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Verantwortlichem und Auftragsverarbeiter auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des

Auftragsverarbeiters und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Verantwortliche berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragsverarbeiter hat die Einhaltung der Pflichten des/der Subunternehmer(s) wie folgt zu überprüfen:

Kontrolle hinsichtlich der Aktualität der TOM und der Liste der Subunternehmer

Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Verantwortlichen auf Verlangen zugänglich zu machen.

Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragsverarbeiter im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Zurzeit sind für den Auftragsverarbeiter die in Anlage 3 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Verantwortliche einverstanden.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).

8. Technische und organisatorische Maßnahmen (insbesondere Art. 28 Abs. 3 Satz 2 lit. c und e DS-GVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Niveau der Sicherheit der Verarbeitung gewährleistet. Dazu werden einerseits mindestens die Schutzziele von Art. 32 Abs. 1 DS-GVO wie **Vertraulichkeit**, **Verfügbarkeit** und **Integrität** der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch

geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird (Art. 28 Abs. 3 lit. c). Die Formulierung in Art. 32 Abs. 1 DS-GVO „diese Maßnahmen schließen unter anderem Folgendes ein“ verdeutlicht andererseits, dass die dort vorgenommene Aufzählung nicht abschließend ist. Für die Auftragsverarbeitung werden daher auch technische und organisatorische Maßnahmen umgesetzt, die die in Kapitel III der DS-GVO genannten Rechte der betroffenen Personen wahren (Art. 28 Abs. 3 lit. e). Diese Maßnahmen stellen u. a. sicher, dass Daten nur für den Zweck verarbeitet und ausgewertet werden können, für den sie erhoben werden (**Zweckbindung**), dass Betroffene, Verantwortliche und Kontrollinstanzen u. a. erkennen können, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden und welche Systeme und Prozesse dafür genutzt werden (**Transparenz**) und dass den Betroffenen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung jederzeit wirksam gewährt werden (**Intervenierbarkeit**). Entsprechend sind auch die Maßnahmenbereiche zu berücksichtigen, die vorrangig der Minimierung der Eingriffsintensität in die Grundrechte Betroffener dienen.

Beispiele für typische, bewährte technische und organisatorische Maßnahmen in den einzelnen Bereichen können den „Hinweisen zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO“ (Abschnitte 6.7 bis 6.9) entnommen werden. Die Auflistung dort ist nicht vollständig oder abschließend. In Abhängigkeit von den konkreten Verarbeitungstätigkeiten können weitere oder andere Maßnahmen geeignet und angemessen sein.

Methodik der Risikobewertung

Für die auftragsgemäße Verarbeitung personenbezogener Daten wird folgende Methodik zur Risikobeurteilung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt:

Interne jährliche Aktualisierung und Bewertung des Verzeichnisses von Verarbeitungstätigkeiten anhand einer Datenschutz-Folgenabschätzungscheckliste.

Das in Anlage 1 beschriebene Datenschutz- und Datensicherheitskonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum Datensicherheitsrisiko unter Berücksichtigung der Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität, Zweckbindung, Transparenz und Intervenierbarkeit detailliert und unter besondere Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragsverarbeiter dar.

Das in Anlange 2 beschriebene Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung wird als verbindlich festgelegt.

Der Auftragsverarbeiter hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (siehe Abschnitt 8) und das Ergebnis samt vollständigem Auditbericht dem Verantwortlichen mitzuteilen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Verantwortlichen abzustimmen.

Soweit die beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen den Anforderungen des Verantwortlichen nicht genügen, benachrichtigt er den Verantwortlichen unverzüglich.

Die Datensicherheitsmaßnahmen beim Auftragsverarbeiter können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Sicherheitsstandards nicht unterschreiten.

Wesentliche Änderungen sind vom Auftragsverarbeiter mit dem Verantwortlichen in dokumentierter Form (schriftlich, elektronisch) abzustimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9. Verpflichtungen des Auftragsverarbeiters nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragsverarbeiter sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen.

Folgende Petitionsdaten verbleiben auf der Plattform von openPetiton:

Petitionen: Petent, Empfänger, Petitionstext, Neuigkeiten, Stellungnahmen

Petitionsunterschriften: Name, Adresse, Datum der Unterschrift.

Die Löschung bzw. Vernichtung sind dem Verantwortlichen mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10. Vergütung

Der Auftragnehmer ist berechtigt für Kontrollen eine angemessene Vergütung vom Auftraggeber zu verlangen.

11. Haftung

Auf Art. 82 DS-GVO wird verwiesen.

12. Vertragsstrafe

Bei Verstoß des Auftragsverarbeiters gegen die Regelungen dieses Vertrages, insbesondere zur Einhaltung des Datenschutzes, wird keine Vertragsstrafe vereinbart.

13. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Verantwortlichen beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen.

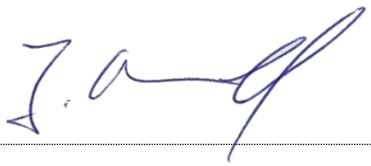
14. Salvatorische Klausel

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Datum:

Unterschriften

Verantwortlicher:



Auftragsverarbeiter: Geschäftsführer Jörg Mitzlaff

Anlage 1: Technische und organisatorische Maßnahmen (TOM)

i.S.d. Art. 32 DSGVO

Organisation:
openPetition gGmbH
Stand:
24.07.2018
Verfasser:
Jörg Mitzlaff
Geschäftsführer openPetition gGmbH
Greifswalder Str. 4, 10405 Berlin

1 Technische und organisatorische Maßnahmen

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die openPetition gGmbH erfüllt diesen Anspruch durch folgende Maßnahmen:

1.1 Zutrittskontrolle

Personenbezogene Nutzerdaten werden ausschließlich auf Servern im Rechenzentrum von Hetzner verarbeitet.
Besucher, Dienstleister und Lieferanten sind nur in Begleitung im Büro.
Die Bürotür ist zu jedem Zeitpunkt verschlossen, der Vermieter hat nachts und am Wochenende einen Wachschutz.
Der Vermieter verwaltet das Schließsystem. Es werden Schlüssel an die Mitarbeiter ausgegeben.
Es gibt eine Vorschrift, wie das Büro gegen Einbruch beim Verlassen zu sichern ist.

1.2 Zugangskontrolle

Die Regeln zur Generierung und Anwendung von Passwörtern ist in den Datenschutzrichtlinien hinterlegt.
Je nach Sicherheitsstufe werden verschiedene Passwortregelungen verwendet. Sie sind in den Datenschutzrichtlinien hinterlegt.

Nach wenigen Minuten ohne Aktivität, aktiviert sich an allen Arbeitsplätzen der automatische Bildschirmschoner mit Passwortschutz.
Für die Anwendungssoftware werden nur personalisierte Zugänge und Passwörter verwendet, allein schon aus Gründen der Nachvollziehbarkeit von Handlungen.
Der Administrator prüft regelmäßig Logs nach Auffälligkeiten.
Der Zugriff auf die Server erfolgt über ein Public-Key-Verschlüsselungsverfahren. Der Zugang ist auf die Mitarbeiter mit der Rolle Administration beschränkt.
Datenträger von Arbeitsplatzrechnern mit personenbezogenen Daten werden auf Dateisystem-Ebene verschlüsselt.
In den Büros sind keine Server und Rechner mit personenbezogenen Daten installiert. Mobile Arbeitsplatzrechner werden im Normalfall nicht im Büro gelagert.
Keine Standard Ports für SSH Verbindungen.
Einsatz von Viren-Schutzprogrammen auf allen Arbeitsplatzrechnern.
Kontrolle der Einhaltung von Standards für sichere Programmierung nach dem 4-Augen Prinzip.
Trennung Produktiv- und Testsystem.
Regelmäßige Prüfung auf bekannte Angriffsvektoren.
Die Webserver-Installation hat nur auf statische Dateien Zugriff.
Restriktive Konfiguration von Webservern.
Minimierung des Einsatzes externer Softwarebibliotheken und Frameworks.
Automatisierte Aktualisierung von Serverbetriebssystem-Updates. Zeitnaher Serverreboot nach Kernel Updates.

1.3 Zugriffskontrolle

Es gibt die Rollen Redaktion, Technik, Administration und Geschäftsführung.
Die Rollen haben je nach Aufgabenprofil zu spezifischen, personenbezogenen Daten, Lese-, Schreib- und Löschrechte. Die Rechte werden von der Anwendungssoftware durchgesetzt.
Nur der Geschäftsführer und Administratoren können Geräte administrieren. Die Administration von Servern und Arbeitsplatzrechnern sind getrennt.
Der Geschäftsführer erteilt Berechtigungen. Das Rechte- und Rollenkonzept ist Teil des Verzeichnisses von Verarbeitungstätigkeiten.
Analoge personenbezogene Daten fallen im Büro nicht an. Werden uns analoge personenbezogene Daten zugesendet, werden sie geschreddert.
Nicht mehr benötigte Datenträger werden physisch zerstört.
Es gibt keine externen Datenträger mit personenbezogenen Daten. Backups erfolgen auf eigenen Servern.
Zu jedem Zeitpunkt ist die Anzahl der abrufbaren personenbezogenen Datensätze durch die Anwendungssoftware beschränkt.

1.4 Weitergabekontrolle

Personenbezogene Daten können über einen Webdienst exportiert werden.
Die Daten sind über ein Nutzeraccount gesichert und werden per SSL Verschlüsselung übertragen.
Es gibt drei Schutzklassen: interne Daten, personenbezogene Daten und geheime Daten wie Passwörter und private Keys.
Die Datenschutzrichtlinie regelt, welche Daten nur verschlüsselt übertragen werden dürfen.
Per Email übertragene Daten werden 10 Jahre lang aufbewahrt.
Durch Firewalls werden die möglichen Kommunikationskanäle auf unseren Servern beschränkt. Es werden die Serverlogs auf auffälligen Webanfragen geprüft und ggf. manuell blockiert.
Der Zugriff auf die Datenbank ist intern über eine verschlüsselte SSL Verbindung realisiert. Externer Datenbank Zugriff ist nur über eine gesicherte SSH Verbindungen möglich.

1.5 Eingabekontrolle

Nachvollziehbarkeit von Eingabe, Änderung und Ausblenden von personenbezogenen Daten durch individuelle Benutzerkonten und Verwendung eines Changelogs auf Anwendungsebene.
Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts.

1.6 Auftragskontrolle

Von allen Auftragsdatenverarbeitern liegen ADV-Verträge vor.
Hostingprovider Hetzner Online ist nach DIN ISO/IEC 27001 zertifiziert.
Die Server sind Root-Serversysteme mit exklusivem root Zugang.
Dienstleistende sind vertraglich an die Befolgung der datenschutzrechtlichen Anweisungen gebunden.
Mitarbeiter sind vertraglich und durch eine Vertraulichkeitserklärung an die Befolgung der datenschutzrechtlichen Anweisungen gebunden.

1.7 Verfügbarkeitskontrolle

Backups des Server-Dateisystems erfolgen täglich. Die Datenbank wird in Echtzeit mit einem Master-Slave Verfahren repliziert.
Backups werden einmal im Quartal zurückgespielt und auf Korrektheit überprüft. Der Status der Datenbank-Replikation wird laufend überprüft.

1.8 Trennungsgebot

Kundendaten werden durch spezifische Datenbankattribute von anderen Datensätzen unterschieden.
Das Datenbankmodell sichert die Trennung von inhaltlich unterschiedlichen Daten.
Kundendaten unterliegen dem gleichen Rollen- und Rechtemodell für personenbezogene Daten.

Test- und Produktivsysteme liegen auf verschiedenen physischen Servern.

1.9 Organisation (Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung)

Der Verantwortliche für die datenschutzkonforme Verarbeitung von Daten nach Artikel 24 DSGVO ist bei openPetition der geschäftsführende Gesellschafter Jörg Mitzlaff.
Der Verantwortliche für die datenschutzkonforme Verarbeitung von Daten nach Artikel 24 DSGVO ist studierter Diplom-Informatiker und hat eine langjährige, einschlägige Berufserfahrung mit informationsverarbeitenden Systemen.
Der Nachweis über die DSGVO-konforme, regelmäßige Verarbeitung personenbezogener Daten nach Art. 30 DSGVO liegt digital als Google-Drive Dokument vor und wird laufend aktualisiert.
Mitarbeiter werden im Umgang mit personenbezogenen Daten geschult. Mitarbeiter protokollieren die Kenntnisnahme der Datenschutzrichtlinien und der Vertraulichkeitsverpflichtung für Mitarbeiter von openPetition.
Das Datenschutzkonzept fasst die Einzelmaßnahmen Verzeichnis von Verarbeitungstätigkeiten, Datenschutz-Folgenabschätzung für neue Produkte und Dienstleistungen, Vertragsmanagement für Auftragsdatenverarbeitung, Datenschutzrichtlinien und Vertraulichkeitsverpflichtung von Mitarbeitern, das Management für die Wahrnehmung von Betroffenenrechten und das Management für die Meldung von Datenschutzverstößen an einem Ort zusammen.
Die Entwicklung orientiert sich am BSI Leitfaden zur Entwicklung sicherer Webanwendungen.
Das Dokument Datenschutzrichtlinien und Vertraulichkeitsverpflichtung für Mitarbeiter von openPetition wird regelmäßig an die neuen technischen Anforderungen im Umgang mit personenbezogenen Daten angepasst.
Datenminimierung personenbezogener Daten ist ein Design-Kriterium bei der Weiterentwicklung und Wartung der Anwendungssoftware.
Der Geschäftsführer ist zugleich der Informationssicherheitsbeauftragte. Grundlage für das Informationssicherheits-Management sind die IT-Grundschutzkataloge des BSI. Das Informationssicherheits-Management fasst die Einzelmaßnahmen Schulung zum sicheren Umgang mit der IT-Infrastruktur, Verwaltung der Zugänge und Zugriffsrechte, Maßnahmenkatalog für die Entwicklung sicherer Webanwendungen, Maßnahmenkatalog für die Absicherung von Standard-Hardware und -Software, Maßnahmenkatalog für Ausfälle und Sicherheitsvorfälle an einem Ort zusammen.

1.10 Datenschutzfreundliche Voreinstellungen

Benutzer haben jederzeit die Möglichkeit, mit wenigen Klicks die Einwilligung in die Speicherung personenbezogener Daten zu widerrufen und ihre Daten zu löschen.
Benutzer haben jederzeit die Möglichkeit, mit wenigen Klicks Auskunft über die von ihm gespeicherten Daten zu erhalten.

Anlage 2: Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutz-Management

Es gelten die Grundsätze:

- Datenschutz ist Aufgabe des gesamten Unternehmens
- Es werden datenschutzfreundliche Technologien eingesetzt, wo immer das möglich und wirtschaftlich ist
- Die IT-Sicherheit muss auf dem aktuellen Stand der Technik sein

Das Unternehmen legt Strategien fest hinsichtlich:

- Zuweisung von Zuständigkeiten
- Risikobewertung
- Durchführung von Kontrollen
- Sensibilisierung und Schulung der Mitarbeiter

Wenn immer das erforderlich ist, werden die eingesetzten Verfahren einer dokumentierten Datenschutz-Folgenabschätzung unterzogen, bestehend aus:

- Schutzbedarfsfeststellung
- Risikoanalyse
- Sicherheitskonzept

Durchgeführte Verarbeitungstätigkeiten – auch als Auftragsverarbeiter – werden einheitlich und nachweisbar dokumentiert.

Weisungen von Kunden im Rahmen einer Auftragsverarbeitung werden kundenbezogen dokumentiert.

Ausgeführte Tätigkeiten im Rahmen der Auftragsverarbeitung werden kundenbezogen dokumentiert.

Alle eingesetzten Auftragsverarbeiter werden eingehenden Prüfungen unterzogen. Dabei werden die gleichen Maßstäbe angesetzt, die für die eigene Verarbeitung gelten.

Incident-Response-Management

Es bestehen interne Richtlinien, Handlungsanweisungen und Prozesse zum Datenschutz, die bei Bedarf oder sich ändernden Voraussetzungen erweitert bzw. ergänzt werden.

Anlage 3: Unterauftragnehmer

der openPetition gGmbH

Der Auftragnehmer beauftragt folgende Unternehmen als Unterauftragnehmer:

Hetzner Online GmbH

Industriestr. 25
91710 Gunzenhausen
www.hetzner.com
info@hetzner.com
Tel.: +49 9831 505-0

Einsatzgebiet: Rechenzentrumsdiensleistungen, für die Prozessierung und Speicherung von Auftraggeberdaten.

Technische und organisatorische Maßnahmen: www.hetzner.com/AV/TOM.pdf
Subunternehmer: www.hetzner.com/AV/subunternehmer.pdf
Datenschutz: www.hetzner.de/rechtliches/datenschutz

Wikando GmbH

Schießgrabenstr. 32
86150 Augsburg
www.fundraisingbox.com
info@fundraisingbox.com
Tel.: +49 (0)82190786255

Einsatzgebiet: Zahlungsabwicklung von Spenden-Transaktionen.

Technische und organisatorische Maßnahmen:
www.fundraisingbox.com/adv/tom.html
Subunternehmer: www.fundraisingbox.com/adv/subcontractor.html
Datenschutz: www.fundraisingbox.com/datenschutz

Stand: 05.2019