Präambel

Die Crowdfox GmbH („**Crowdfox**“) und der Kunde schließen einen Vertrag über SaaS-Leistungen („**Hauptvertrag**“) und sind darüber übereingekommen, dass dieser Vertrag zur Auftragsverarbeitung („**AVV**“) als Anhang zum Hauptvertrag Bestandteil des Hauptvertrags wird. Mit Wirksamkeit des Hauptvertrags tritt dieser Vertrag in Kraft und Bedarf zur Wirksamkeit keiner weiteren Unterschrift. Rechte und Pflichten aus diesem Vertrag leiten sich nur ab, soweit der Kunde mit Crowdfox den Hauptvertrag abgeschlossen hat.

Inhaltsübersicht

I. Allgemeine Regelungen

1. Crowdfox verarbeitet als Auftragsverarbeiter („Auftragnehmer“) für den Kunden als Verantwortlichen („Auftraggeber“, gemeinsam „Parteien“) personenbezogene Daten in der in diesem Vertrag beschriebenen Art im Auftrag des Verantwortlichen unter Beachtung nachfolgender Regelungen.
2. Dieser AVV regelt die Rechte und Pflichten der Parteien im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag. Dieser AVV ist so konzipiert, dass er den Bestimmungen der geltenden Datenschutz-Grundverordnung („DSGVO“), dem Bundesdatenschutzgesetz und den einschlägigen Landesdatenschutzgesetzen gerecht wird.
3. Dieser AVV findet auf solche Tätigkeiten Anwendung, bei denen der Auftragnehmer, Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer personenbezogene Daten des Auftraggebers im Kontext des Hauptvertrags im Sinne von Art. 28 DSGVO verarbeiten.
4. In diesem AVV verwendete Begriffe sind entsprechend ihrer Definition in der DSGVO zu verstehen.
5. Diese Vereinbarung ersetzt sämtliche vorherigen Datenschutzvereinbarungen und AV- bzw. ADV-Verträge zwischen den Parteien.
6. Bei Widersprüchen zwischen dem Hauptvertrag und diesem AVV, geht der AVV in datenschutzrechtlichen Belangen als speziellere Regelung vor.

II. Zweck der Verarbeitung und der Art der personenbezogenen Daten

Crowdfox verarbeitet im Rahmen des Leistungsumfangs aus dem Hauptvertrag folgende personenbezogenen Daten:

- Kommunikationsdaten (z.B. E-Mail Adresse),
- Nutzerdaten (z.B. IP-Adresse)
- geschäftliche Adressdaten der Nutzer (z.B. Adresse eines Standortes)

III. Verarbeitungstätigkeiten

Verarbeitungstätigkeit ist die Speicherung der personenbezogenen Daten zur Erfüllung der Pflichten aus dem Hauptvertrag.

IV. Kategorien betroffener Personen

Betroffenen Personen sind Mitarbeiter des Auftraggebers.

V. Pflichten des Auftraggebers

1. Der Auftraggeber ist im Rahmen dieses AVV für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Verarbeitung allein verantwortlich. Dies gilt auch im Hinblick auf den in dieser Vereinbarung geregelten Gegenstand, Umfang, Art und Zweck der Datenverarbeitung, die Beschreibung der betroffenen Daten gemäß Ziffer 1.2 und die Wahrung der Betroffenenrechte.
2. Insbesondere trägt der Auftraggeber die Verantwortung dafür, dass die vom

Auftragnehmer für diese Verarbeitung getroffenen technischen und organisatorischen Maßnahmen („TOM“) für die Risiken der verarbeiteten Daten ein angemessenes Schutzniveau bieten. Der Auftragnehmer ist seinerseits dafür verantwortlich, diese TOM einzuhalten.

3. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er im Hinblick auf die Verarbeitung bezüglich datenschutzrechtlicher Bestimmungen Fehler oder Unregelmäßigkeiten feststellt.

4. Der Auftraggeber nennt dem Auftragnehmer bei Bedarf den Ansprechpartner für im Rahmen dieser AVV anfallende Datenschutzfragen.

5. Weitere Rechte und Pflichten ergeben sich aus den nachfolgenden Regelungen dieser AVV und der DSGVO sowie den dazugehörigen gesetzlichen Bestimmungen.

VI. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

1. Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.

2. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

3. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, Art. 32 DSGVO.

4. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

5. Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

6. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

7. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen

und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

8. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber.

VII. Technisch-organisatorische Maßnahmen

1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen ist der Auftragsnehmer verpflichtet, geeignete technische und organisatorische Maßnahmen („**TOM**“) zu treffen, und zwar auf eine Art und Weise, dass die Verarbeitung personenbezogener Daten die Anforderungen des anwendbaren Datenschutzrechts, insbesondere der DSGVO und dieses Vertrags, erfüllt.

2. Zu diesem Zweck und nach Maßgabe von Artikel 32 DSGVO hat der Auftragnehmer die spezifischen Maßnahmen angemessen zu dokumentieren und auf Verlangen des Auftraggebers vorzulegen.

3. Die TOM ändern sich mit dem technischen Fortschritt und werden beständig weiterentwickelt. In diesem Zusammenhang darf der Auftragsverarbeiter geeignete alternative Maßnahmen ergreifen. Das Sicherheitsniveau der genannten Maßnahmen darf jedoch nicht ohne Zustimmung des Auftraggebers unter das in diesem Vertrag vereinbarte Niveau sinken.

4. Die vom Auftragnehmer zum Zeitpunkt dieses Datenschutzvertrags implementierten TOM sind in Anhang 1 zu diesem AVV aufgeführt.

VIII. Transfer von personenbezogenen Daten

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen des Art. 44 ff. DSGVO erfüllt sind. Sollten diese Anforderungen erfüllt sein, müssen jedoch wichtige datenschutzrechtliche Gründe vorliegen, um die Zustimmung zu verweigern.

IX. Unterauftragsverhältnisse

1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen und dabei personenbezogene Daten verarbeiten. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der

Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

2. Die Beauftragung von Unterauftragnehmern bei der Verarbeitung oder Nutzung personenbezogener Daten ist grundsätzlich nur mit einer Genehmigung vom Auftraggeber gestattet. Für die zum Zeitpunkt des Vertragsschlusses in der in Anhang 2 aufgeführten Unterauftragnehmer gilt diese Genehmigung als erteilt. Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Unterauftragnehmer in Anspruch zu nehmen. Er kann jedoch gegen derartige Änderungen Einspruch erheben, wobei dies nicht ohne wichtigen datenschutzrechtlichen Grund erfolgen darf. Der Auftragnehmer informiert den Auftraggeber in Textform durch aktive Mitteilung (z.B. E-Mail), wenn er die Hinzuziehung weiterer oder die Ersetzung von Unterauftragnehmer beabsichtigt. Der Einspruch gegen die beabsichtigte Änderung ist innerhalb von 14 Tagen nach Bereitstellung der Information über die Änderung gegenüber dem Auftragnehmer in Textform zu erheben (z.B. an datenschutz@crowdfox.com). Im Falle des Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder - sofern die Erbringung der Leistung ohne die beabsichtigte Änderung für den Auftragnehmer nicht zumutbar ist - die Leistung gegenüber dem Auftraggeber innerhalb von 4 Wochen nach Zugang des Einspruchs einstellen und die Hauptvertrag fristlos und mit sofortiger Wirkung kündigen.

3. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

4. Erteilt der Auftragnehmer Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, ihre datenschutzrechtlichen Pflichten aus diesem Vertrag auf die Unterauftragnehmer zu übertragen und eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO mit diesen abzuschließen. Insbesondere gewährleistet der Auftragnehmer, dass die TOM des Unterauftragnehmers dem Schutzniveau der TOM aus diesem AVV genügen.

X. Auskunfts- und Kontrollrechte des Auftraggebers

1. Der Auftraggeber hat das Recht Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

2. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

3. Für die Ermöglichung von Kontrollen durch den Auftraggeber wird vereinbart, dass beide Parteien die für die Kontrolle anfallenden personellen Kosten selbst tragen. Die Kosten für vom Auftraggeber berufene Prüfer dritter Parteien werden im gesamten vom Auftraggeber

getragen.

4. Der Auftragnehmer hat das Recht die anlasslose Vor-Ort-Kontrolle abzulehnen, wenn und solange er den Nachweis über die Erfüllung seiner Pflichten, insbesondere die Umsetzung der TOM sowie ihrer Wirksamkeit, durch geeignete Nachweise erbringt. Geeignete Nachweise können insbesondere genehmigte Verhaltensregeln im Sinne von Art. 40 DSGVO oder ein genehmigtes Zertifizierungsverfahren im Sinne von Art. 42 DSGVO sein. Beide Parteien einigen sich darauf, dass auch die Vorlage von Testaten oder Berichten unabhängiger Instanzen (z.B. IT-Sicherheitsbeauftragter, Datenschutzbeauftragter), ein schlüssiges Datensicherheitskonzept oder eine geeignete Zertifizierung durch ein IT-Sicherheits- und Datenschutzaudit als geeignete Nachweise anerkannt werden.

XI. Mitteilung bei Verstößen des Auftragnehmers

1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.:
   - die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
   - die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
   - die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
   - die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

2. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

XII. Weisungsbefugnis des Auftraggebers

1. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Der Auftragnehmer haftet nicht, sofern das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird und dies einzig von diesem verschuldet ist.

2. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der

Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

XIII. Löschung und Rückgabe von personenbezogenen Daten

1. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
2. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Hauptvertrag – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
3. Dokumentationen, die dem Nachweis der Auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

XIV. Haftung

1. Auf Art. 82 DSGVO wird verwiesen.
2. In allen anderen Fällen haftet der Auftraggeber im Innenverhältnis voll für den Schaden und stellt den Auftragnehmer von etwaigen Ansprüchen des Betroffenen oder Dritten auf erste Anforderung frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftragnehmer erhoben werden.
3. Der Auftraggeber trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstands ist.
4. Jegliche Haftungsausschlüsse in diesem Vertrag gelten nicht im Falle von Vorsatz und grober Fahrlässigkeit sowie bei Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit.

XV. Laufzeit des AVV

Die Laufzeit dieses AVV entspricht der Laufzeit des Hauptvertrags.

XVI. Sonstige Bestimmungen

Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - sind gemäß DSGVO schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

XVII. Anhänge

Anhang 1: Technisch-Organisatorische Maßnahmen

Anhang 2: Unterauftragsverhältnisse

Crowdfox GmbH
Im Mediapark 8a
50670 Köln
GF: Dirk Schäfer

Telefon:
+49 221 165359-38
professional@crowdfox.com
www.crowdfox.pro

Bank:
Commerzbank Bergisch Gladbach
IBAN: DE42370400440277726600
BIC: COBADEFFXXX

Steuernummer: DE297246515
Amtsgericht: Köln, HRB 81982
Sitz der Gesellschaft:
Deutschland, Köln

Anhang 1: Technisch-organisatorische Maßnahmen

Vertraulichkeit

Unter die Vertraulichkeit fallen die Punkte „Zutrittskontrolle“, „Zugangskontrolle“, „Zugriffskontrolle“ und „Trennungskontrolle“

- **Zutrittskontrolle**
  Unter Zutrittskontrollen sind Maßnahmen zu verstehen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Maßnahmen	Organisatorische Maßnahmen
Alarmanlage	Schlüsselregelung/Liste
Automatisches Zugangskontrollsystem	Empfang/Rezeption/Pförtner
Biometrische Zugangssperren	Besucherbuch/Protokoll der Besucher
Chipkarten/Transpondersysteme	Sorgfalt bei Auswahl Reinigungsdienste
Manuelles Schließsystem	Besucher in Begleitung durch Mitarbeiter
Sicherheitsschlösser	Sorgfalt bei Auswahl des Wachpersonals
Schließsystem mit Codesperre	
Türen mit Knauf Außenseite	
Klingelanlage mit Kamera	
Videoüberwachung der Eingänge	

- **Zugangskontrolle**
  Unter Zugangskontrollen sind Maßnahmen zu verstehen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint.

Technische Maßnahmen	Organisatorische Maßnahmen
Login mit Benutzername und Passwort	Verwalten von Benutzerberechtigungen
Automatische Desktopsperre	Erstellen von Benutzerprofilen
Anti-Viren-Software Server	Zentrale Passwortvergabe
Anti-Virus-Software Clients	Richtlinie „Sicheres Passwort“
Anti-Virus-Software mobile Geräte	Richtlinie „Löschen/Vernichten“
Firewall	Richtlinie „Clean desk“
Intrusion Detection Systeme	Allg. Richtlinie Datenschutz und/oder Sicherheit
Mobile Device Management	Mobile Device Policy
Einsatz VPN bei Remote-Zugriffen	
Verschlüsselung von Datenträgern	
Verschlüsselung von Notebooks/Tablet	

- **Zugriffskontrolle**
  Unter Zugriffskontrollen sind Maßnahmen zu verstehen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
Aktenschredder (mind. Stufe 3, cross cut)	Einsatz Berechtigungskonzepte
Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	Zugriffsrechte werden nicht direkt vergeben, sondern bestimmten Benutzergruppen werden die notwendigen Rechtegruppen zugeordnet
Physische Löschung von Datenträgern	Minimale Anzahl an Administratoren
	Verwaltung der Benutzerrechte durch Administratoren

- **Trennungskontrolle**
  Unter Trennungskontrollen sind Maßnahmen zu verstehen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
Trennung von Produktiv- und Testumgebung	Steuerung über Berechtigungskonzept
Physikalische Trennung (Systeme/Datenbanken / Datenträger)	Festlegung von Datenbankrechten
Mandantenfähigkeit relevanter Anwendungen	Kategorisierung von Datenarten

Pseudonymisierung

Unter Pseudonymisierung versteht man die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Organisatorische Maßnahmen
Interne Anweisung, personenbezogene Daten möglichst zu anonymisieren/ pseudonymisieren

Integrität

Unter den Punkt der Integrität fallen die „Weitergabekontrolle“ und „Eingabekontrolle“.

- **Weitergabekontrolle**

  Unter Weitergabekontrolle sind Maßnahmen zu verstehen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen	Organisatorische Maßnahmen
Email-Verschlüsselung	Weitergabe in anonymisierter oder pseudonymisierter Form
Einsatz von VPN	Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
Protokollierung der Zugriffe und Abrufe	
Bereitstellung über verschlüsselte Verbindungen wie sftp, https	

- **Eingabekontrolle**

  Unter Eingabekontrolle sind Maßnahmen zu verstehen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Technische Maßnahmen	Organisatorische Maßnahmen
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
Manuelle oder automatisierte Kontrolle der Protokolle	Klare Zuständigkeiten für Löschungen
	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitung übernommen wurden

Verfügbarkeit und Belastbarkeit

- **Verfügbarkeits- und Belastbarkeitskontrolle**

Unter Verfügbarkeitskontrolle sind Maßnahmen zu verstehen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen	Organisatorische Maßnahmen
Feuer- und Rauchmeldeanlagen	Backup & Recovery-Konzept (ausformuliert)
Feuerlöscher Serverraum	Kontrolle des Sicherungsvorgangs
Serverraumüberwachung Temperatur und Feuchtigkeit	Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
Serverraum klimatisiert	Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
USV	Getrennte Partitionen für Betriebssysteme und Daten
Schutzsteckdosenleisten Serverraum	Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
RAID System / Festplattenspiegelung	
Videoüberwachung Serverraum	
Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- **Datenschutz-Management**

Technische Maßnahmen	Organisatorische Maßnahmen
Software-Lösungen für Datenschutz-Management im Einsatz	Externer Datenschutzbeauftragter: Christian Volkmer Projekt 29 GmbH & Co. KG Ostengasse 5 93047 Regensburg Tel.: 0941-298693-0 Fax: 0941-298693-16 Mail: info@projekt29.de Web: www.projekt29.de
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung	Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet

Sicherheitszertifizierung nach ISO 27001	Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	Externer CISO: Christian Volkmer Projekt 29 GmbH & Co. KG Ostengasse 5 93047 Regensburg Tel.: 0941-298693-0 Fax: 0941-298693-16 Mail: info@projekt29.de Web: www.projekt29.de
	Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
	Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach

- **Incident-Response-Management**
  Unterstützung bei der Reaktion auf Sicherheitsverletzungen.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Einsatz von Firewall und regelmäßige Aktualisierung	Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Daten-pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
Einsatz von Spamfilter und regelmäßige Aktualisierung	Dokumentierte Vorgehensweise zu Umgang mit Sicherheitsvorfällen
Einsatz von Virenscanner und regelmäßige Aktualisierung	Einbindung von DSB und CISO in Sicherheitsvorfälle und Datenpannen
Intrusion Detection System (IDS)	Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
Intrusion Prevention System (IPS)	Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

- **Datenschutzfreundliche Voreinstellungen**
  Privacy by design / Privacy by default.

Technische Maßnahmen

Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

- **Auftragskontrolle (Outsourcing an Dritte)**
  Unter Auftragskontrolle sind Maßnahmen zu verstehen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Organisatorische Maßnahmen
Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard Vertragsklauseln
Schriftliche Weisungen an den Auftragnehmer
Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
Regelung zum Einsatz weiterer Subunternehmer
Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Anhang 2: Unterauftragsverhältnisse

Folgende Unterauftragnehmer können durch Crowdfox damit beauftragt sein, personenbezogene Daten im Verantwortungsbereich der Crowdfox Kunden zu verarbeiten.

Der Zweck der Verarbeitung, die Verarbeitungstätigkeit, die Kategorien betroffener Personen und die Kategorien der personenbezogenen Daten ergeben sich aus dem AVV, soweit sich aus dieser Übersicht nichts anderes ergibt.

Unterauftragnehmer	**Anschrift**	**Leistung**
firstcolo GmbH	Kruppstraße 105, 60388 Frankfurt am Main	Bereitstellung von Rechenzentren, Serverhosting
Microsoft Ireland Operations Ltd.	One Microsoft Place South County Business Park Leopardstown Dublin 18 D18 P521, Ireland	Bereitstellung von Rechenzentren, Serverhosting
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy 1855 Luxembourg	Bereitstellung von Rechenzentren, Serverhosting