social matching
Dein Jobportal für das Sozialwesen

Auftragsverarbeitungsvertrag (AVV) gemäß Art 28 Abs 3 DSGVO

Diese Vereinbarung bildet eine Ergänzung zum Vertrag (nachfolgend "Hauptvertrag") und

wird zwischen

Kunde (nachfolgend "Verantwortlicher")

siehe
Hauptvertrag
Deutschland

und

Social Matching Plattformen GmbH (nachfolgend "Auftragsverarbeiter")

Obergrombacher Straße 13
76646 Bruchsal
Deutschland

(beide Parteien gemeinsam nachfolgend "Vertragsparteien")

geschlossen.

Mit dem Abschluss dieser Vereinbarung gehen die Vertragsparteien ein Auftragsverarbeitungsverhältnis ein. In dieser Vereinbarung gelten die entsprechenden Begriffsdefinitionen der DSGVO (Datenschutz-Grundverordnung - Verordnung (EU) 2016/679). Wenn daher in diesem Vertragswerk etwa der Begriff „Daten“ verwendet wird, dann sind damit „personenbezogene Daten“ im Sinne der DSGVO gemeint. Falls sich diese Vereinbarung und der Hauptvertrag bezüglich der Verarbeitung von personenbezogenen Daten widersprechen, geht diese Vereinbarung im Zweifel dem Hauptvertrag vor.

§ 1: Vertragsgegenstand und Dauer des Vertrages

1.1. : Dieser Vertrag findet Anwendung auf all jene Verarbeitungen personenbezogener Daten, die sich aus dem Hauptvertrag zwischen den Vertragsparteien ergeben, sofern der Auftragsverarbeiter diese personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet.

1.2. : Der Auftragsverarbeitungsvertrag tritt ab dem Zeitpunkt der Unterfertigung durch beide Parteien in Kraft. Er gilt akzessorisch zum Hauptvertrag und bleibt jedenfalls für die Dauer der datenschutzrechtlich relevanten Leistungserbringung aus dem Hauptvertrag in Geltung. Bei vollständigem Wegfall des Hauptvertrages erlischt auch diese Vereinbarung automatisch. Es bedarf in diesem Fall keiner gesonderten Kündigung.

1.3. : Dieser Vertrag und somit das gesamte Auftragsverarbeitungsverhältnis kann von den Vertragsparteien zu jeder Zeit ohne Einhaltung einer Frist aufgekündigt werden, wenn die jeweils andere Partei schwerwiegend gegen

diese Vereinbarung oder das einschlägige Datenschutzrecht verstößt.

1.4. : Gegenstand der Auftragsverarbeitung sind die Erhebung, Verarbeitung und Weitergabe von personenbezogenen Daten von Personen, die sich für die (Stellen-)Angebote des Auftraggebers interessieren und in Folge darauf bewerben. Die Erhebung solcher Daten erfolgen durch aktive und passive Recruitingmaßnahmen durch den Auftraggeber (Direktansprache, Social-Media-Werbeanzeigen und -Kampagnen, über die Homepage (https://socialmatching.de), und vergleichbare Kanäle und Maßnahmen, im Sinne zur (Vermittlungs-)Zielerreichung für den Auftragverarbeiter. Die bezeichneten Daten werden zu diesem Zweck - unter Einhaltung der geltenden Datenschutzbestimmungen - von dem Auftraggeber an den Auftragverarbeiter, inkl. zugehöriger Datenschutzverpflichtungen, übertragen. Die sich bewerbende Person stimmt dieser Weitergabe aktiv zu.

- Die Auftragsverarbeitung erfolgt im Rahmen der folgenden Rechtsbeziehung (Hauptvertrag): Pilotkundenvertrag und/ oder Kundenvertrag und/ oder Bildungseinrichtungsvertrag
- Detailangaben zum Gegenstand der im Auftrag erfolgenden Verarbeitung, die verarbeiteten personenbezogenen Daten, von der Verarbeitung betroffene Personen sowie Art, Umfang und Zweck der Verarbeitung, richten sich nach den Vorgaben des Anhangs "**Vertragsgegenstand und Dauer des Vertrages**".

Solch ein schwerwiegender Verstoß ist etwa dann gegeben, wenn der Auftragsverarbeiter die Pflichten, die sich aus dieser Vereinbarung und aus dem Art 28 DSGVO ergeben, nicht einhält. Weiters kann der Verantwortliche fristlos kündigen, wenn der Auftragsverarbeiter eine Weisung des Verantwortlichen nicht befolgt, wenn der Auftragsverarbeiter die vertragsmäßig festgelegten Kontrollrechte des Verantwortlichen verweigert oder wenn der Auftragsverarbeiter zwingend notwendige oder vereinbarte Sicherheitsmaßnahmen unterlässt.

§ 2: Art und Zweck der Verarbeitung

2.1. : Die personenbezogenen Daten, die vom Verantwortlichen zur Verfügung gestellt werden, verarbeitet der Auftragsverarbeiter ausschließlich zur Erfüllung seiner vertraglichen Pflichten aus dem Hauptvertrag. Die Verarbeitung erfolgt daher aufgrund des Hauptvertrages, dieser Vereinbarung oder gemäß einer Weisung des Verantwortlichen. Dem Auftragsverarbeiter ist es untersagt personenbezogene Daten für eigene oder fremde Zwecke zu verarbeiten oder personenbezogene Daten, ohne vorherige schriftliche Weisung des Verantwortlichen an Dritte weiterzugeben. Die Duplizierung oder Kopie von personenbezogenen Daten durch den Auftragsverarbeiter ist nur so weit erlaubt, als diese im Vorhinein durch den Verantwortlichen genehmigt wurde oder diese für die Sicherstellung der ordnungsgemäßen Datenverarbeitung (Kopie zur Sicherung) oder zur Einhaltung gesetzlicher Pflichten (zB gesetzliche Aufbewahrungspflichten) unbedingt notwendig ist.

2.2. : Die konkreten Verarbeitungsarten (Art 4 Z 2 DSGVO) und Zwecke der Verarbeitung des Auftragsverarbeiters sind dem Hauptvertrag zu entnehmen.

2.3. : Soweit der Auftraggeber als Verantwortlicher der Auftragsverarbeitung handelt, ist er im Rahmen dieses Auftragsverarbeitungsvertrages für die Einhaltung der Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenverarbeitung sowie für die Rechtmäßigkeit der Beauftragung des Auftragsverarbeiters verantwortlich. Soweit der Auftraggeber selbst als Auftragsverarbeiter handelt, beauftragt er den Auftragsverarbeiter als Unterauftragsverarbeiter. Der Verantwortliche der Verarbeitung darf sich auf Grundlage dieses Auftragsverarbeitungsvertrages unmittelbar auf die, dem Auftraggeber gegenüber dem Unterauftragsverarbeiter zustehenden Rechte berufen.

§ 3: Art der personenbezogenen Daten, Kategorien betroffener Personen

Die durch den Auftragsverarbeiter verarbeiteten Arten personenbezogener Daten sowie die Kategorien der betroffenen Personen finden sich in Anhang 1. Der Anhang 1 stellt einen Teil dieser Vereinbarung dar.

§ 4: Rechte und Pflichten des Verantwortlichen

4.1.: Dem Verantwortlichen obliegt allein die Entscheidung über die Mittel und Zwecke der Verarbeitung von den von ihm zur Verfügung gestellten personenbezogenen Daten.

4.2.: Der Verantwortliche verpflichtet sich die EU-rechtlichen und nationalen Datenschutzbestimmungen sowie diese Vereinbarung einzuhalten. Er ist insbesondere dafür verantwortlich, die Rechtmäßigkeit der Verarbeitung personenbezogener Daten (Art 6 DSGVO) zu beurteilen und dass die Rechte der betroffenen Personen gemäß den Art 12 – 22 DSGVO gewahrt werden. Gleichzeitig obliegt die Entscheidung über die Beantwortung einer Anfrage einer betroffenen Person bezüglich ihrer Betroffenenrechte ausschließlich dem Verantwortlichen und die entsprechende Kommunikation erfolgt nur durch diesen.

4.3.: Der Verantwortliche ist berechtigt dem Auftragsverarbeiter Weisungen und Aufträge bezüglich Art und Umfang der Verarbeitung personenbezogener Daten zu erteilen.

Diese Aufträge und Weisungen sind durch den Verantwortlichen grundsätzlich auf eine dokumentierte und schriftliche oder elektronische Weise zu erteilen. Wenn Weisungen mündlich erteilt werden, sind diese schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Unter einer Weisung versteht dieses Vertragswerk eine Anordnung an den Auftragsverarbeiter bezüglich des Umgangs mit personenbezogenen Daten.

4.4.: Datenträger oder Datensätze, die der Verantwortliche dem Auftragsverarbeiter überlässt, verbleiben im Eigentum des Verantwortlichen. Der Verantwortliche ist jederzeit berechtigt dem Auftragsverarbeiter die Löschung, Berichtigung, Herausgabe, Anpassung oder Einschränkung der Datenverarbeitung anzuordnen.

4.5.: Der Verantwortliche meldet dem Auftragsverarbeiter unverzüglich Fehler und Auffälligkeiten, die ihm an Ergebnissen der Auftragsverarbeitung auffallen.

4.6.: Der Verantwortliche ist verpflichtet den Auftragsverarbeiter unverzüglich zu verständigen, wenn es zu einem Wechsel des Datenschutzbeauftragten kommt.

§ 5: Pflichten des Auftragsverarbeiters

5.1.: Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur aufgrund der dokumentierten Weisung des Verantwortlichen, sofern der Auftragsverarbeiter nicht durch das Recht der Union oder der Mitgliedstaaten hierzu verpflichtet ist. 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.

5.2.: Der Auftragsverarbeiter ist verpflichtet personenbezogene Daten zu löschen, zu berichtigen, herauszugeben, anzupassen oder einzuschränken, wenn dies vom Verantwortlichen angeordnet wird.

5.3. : Der Auftragsverarbeiter hat zu gewährleisten, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

5.4. : Der Auftragsverarbeiter verpflichtet sich alle technischen und organisatorischen Maßnahmen (TOMs) im Sinne des Art 32 DSGVO, die für die Sicherheit der Verarbeitung von personenbezogenen Daten erforderlich sind, zu ergreifen. Die durch den Auftragsverarbeiter gesetzten TOMs sind im Anhang 2 näher beschrieben. Der Anhang 2 stellt einen Teil dieser Vereinbarung dar.

5.5. : Der Verantwortliche erklärt sich mit den im Anhang 3 gelisteten weiteren Auftragsverarbeitern (nachfolgend „Sub-Auftragsverarbeiter) einverstanden. Diese gelisteten Sub-Auftragsverarbeiter sind zur Erfüllung des Hauptvertrages erforderlich. Ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung nimmt der Auftragsverarbeiter keine weiteren Auftragsverarbeiter in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung ist der Auftragsverarbeiter verpflichtet, den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Sub-Auftragsverarbeiter zu informieren. Der Verantwortliche hat dann die Möglichkeit gegen die Änderung innerhalb einer angemessenen Frist Einspruch zu erheben.

5.6. : Mit beauftragten Sub-Auftragsverarbeitern wird durch den Auftragsverarbeiter eine vertragliche Vereinbarung geschlossen, die zumindest das gleiche Datenschutzniveau wie dieser Vertrag zwischen dem Verantwortlichen und Auftragsverarbeiter gewährleistet. Dabei werden alle gesetzlichen und vertraglichen Vorgaben berücksichtigt, insbesondere die technischen und organisatorischen Maßnahmen gemäß Art 32 DSGVO.

5.7. : Verstößt ein Sub-Auftragsverarbeiter gegen seine datenschutzrechtlichen Pflichten, haftet der Auftragsverarbeiter dem Verantwortlichen für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters. Der Verantwortliche kann im Falle eines Verstoßes gegen datenschutzrechtliche Pflichten durch den Sub-Auftragsverarbeiter den Auftragsverarbeiter anweisen die Beschäftigung des Sub-Auftragsverarbeiters ganz oder teilweise zu beenden.

5.8. : Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit, damit dieser die Rechte der betroffenen Person nach Kapitel III der DSGVO innerhalb der gesetzlichen Fristen erfüllen kann. Dafür ergreift der Auftragsverarbeiter technische und organisatorische Maßnahmen. Wird ein Antrag irrtümlicherweise an den Auftragsverarbeiter gestellt und ist es ersichtlich, dass er eigentlich an den Verantwortlichen gestellt werden hätte sollen, so leitet der Auftragsverarbeiter den Antrag unverzüglich an den Verantwortlichen weiter und benachrichtigt diesen auch.

5.9. : Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung der in Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgenabschätzung, vorherige Konsultation der Aufsichtsbehörde).

5.10. : Der Auftragsverarbeiter verpflichtet sich nach Erbringung der Verarbeitungsleistungen oder davor nach Anordnung des Verantwortlichen, spätestens mit Beendigung des Hauptvertrages alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben und vorhandene Kopien zu löschen.

Der Auftragsverarbeiter ist berechtigt Dokumentationen, unter Berücksichtigung der einschlägigen Aufbewahrungsfristen, für den Nachweis der auftrags- und ordnungsgemäßen Datenvereinbarung auch nach

Beendigung des Vertragsverhältnisses aufzubewahren.

5.11. : Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Verantwortliche selbst oder durch Dritte Überprüfungen und Inspektionen bezüglich der Einhaltung der Vorschriften über Datenschutz und Datensicherheit beim Auftragsverarbeiter durchführt. Der Auftragsverarbeiter stellt alle dafür erforderlichen Informationen zur Verfügung und wirkt unterstützend mit. Der Verantwortliche hat für diese Überprüfungen und Inspektionen grundsätzlich einen Termin zu vereinbaren. Der Verantwortliche darf seine Kontrollrechte nur in einem angemessenen und erforderlichen Umfang ausüben.

5.12. : Der Auftragsverarbeiter informiert den Verantwortlichen umgehend, wenn es zu schwerwiegenden Störungen des Betriebsablaufes kommt, wenn er der Ansicht ist, dass eine Weisung gegen gesetzliche Datenschutzbestimmungen verstößt, es zu Verstößen durch Mitarbeiter oder Sub-Auftragsverarbeiter kommt oder wenn sich Unregelmäßigkeiten im Zuge der Verarbeitung der Daten des Verantwortlichen ergeben. Der Auftragsverarbeiter kann die Durchführung von Weisungen, die gegen gesetzliche Datenschutzbestimmungen verstoßen, aussetzen, bis sie durch den Verantwortlichen bestätigt oder abgeändert wurden.

5.13. : Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorgaben und der Regelungen dieses Auftragsverarbeitungsvertrag, insbesondere der TOMs beim Auftragsverarbeiter jederzeit im erforderlichen Umfang selbst oder durch Dritte zu kontrollieren und die erforderlichen Überprüfungen, einschließlich Inspektionen, durchzuführen.

5.14. : Der Auftragsverarbeiter hat den Auftraggeber bei den Kontrollen und Inspektionen im erforderlichen Rahmen zu unterstützen (z. B. durch Bereitstellung von Personal und Gewährung von Zugangs- und Zugriffsrechten).

5.15. : Vor-Ort-Kontrollen erfolgen innerhalb üblicher Geschäftszeiten, sind vom Auftraggeber mit einer angemessenen Frist (mindestens 14 Tage) anzumelden. In Notfällen, d. h., wenn ein Zuwarten die Rechte der Betroffenen und/oder des Auftraggebers für diese in einem nicht zumutbaren Maße gefährden würde, kann eine angemessen kürzere Frist gewählt werden. Umgekehrt kann eine längere Frist erforderlich sein (wenn z. B. umfangreiche Vorbereitungen erfolgen müssen oder während der Urlaubszeit). Die Abweichungen von der Frist sind jeweils von der sie in Anspruch nehmenden Vertragspartei zu begründen.

5.16. : Die Kontrollen sind auf den erforderlichen Rahmen beschränkt und müssen auf Betriebs- und Geschäftsgeheimnisse des Auftragsverarbeiters sowie den Schutz von personenbezogenen Daten Dritter (z. B. anderer Kunden oder Mitarbeiter des Auftragsverarbeiters) Rücksicht nehmen. Vermeidbare Betriebsstörungen sind zu vermeiden. Soweit dem Anlass und Zweck der Prüfung genügend, soll sich eine Kontrolle auf Stichproben beschränken.

5.17. : Zur Durchführung der Kontrolle sind nur fachkundige Personen zugelassen, die sich legitimieren können und im Hinblick auf die Betriebs- und Geschäftsgeheimnisse sowie interne Prozesse des Auftragsverarbeiters und personenbezogene Daten zur Vertraulichkeit- und Verschwiegenheit verpflichtet sind. Der Auftragsverarbeiter kann den Nachweis einer entsprechenden Verpflichtung verlangen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragsverarbeiter stehen oder sonst ein begründeter Anlass zur seiner Ablehnung vorliegen, hat der Auftragsverarbeiter gegen diesen ein Einspruchsrecht.

5.18. : Statt der Einsichtnahmen und der Vor-Ort-Kontrollen, darf der Auftragsverarbeiter den Auftraggeber auf eine gleichwertige Kontrolle durch unabhängige Dritte (z. B. neutrale Datenschutzauditoren), Einhaltung genehmigter Verhaltensregeln (Art. 40 DSGVO) oder geeignete Datenschutz-oder IT-Sicherheitszertifizierungen gem. Art. 42 DSGVO verweisen. Dies gilt nur, wenn der Verweis dem Auftraggeber zuzumuten ist und die Art sowie Umfang der Prüfung und Verweise der Art und dem Umfang des berechtigten Kontrollvorhabens des Auftraggebers entsprechen. Der Auftragsverarbeiter verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln gemäß Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung gemäß Art. 42 Abs. 7 und jede

andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.

5.19. : Der Auftraggeber übt sein Kontrollrecht grundsätzlich nicht häufiger als alle 12 Monate aus, es sei denn ein konkreter Anlass (insbesondere eine Verletzung des Datenschutzes, ein Sicherheitsvorfall oder das Ergebnis einer Auditierung) macht Kontrollen vor Ablauf dieses Zeitraums erforderlich.

§ 6: Pflichten des Auftraggebers

6.1. : Der Auftraggeber hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen, Weisungen oder Verarbeitungsprozessen Fehler oder Unregelmäßigkeiten im Hinblick auf datenschutzrechtliche Bestimmungen feststellt.

6.2. : Die Auftraggeber benennt die zum Empfang von Weisungen berechtigte Ansprechpartner und ist verpflichtet Änderungen der Ansprechpartner oder deren Kontaktinformationen sowie Vertreter im Fall einer nicht vorübergehenden Abwesenheit oder Verhinderung unverzüglich mitzuteilen.

6.3. : Im Falle einer Inanspruchnahme des Auftragsverarbeiters durch betroffene Personen, dritte Unternehmen, Stellen oder Behörden hinsichtlich etwaiger Ansprüche aufgrund der Verarbeitung von personenbezogenen Daten im Rahmen dieses Auftragsverarbeitungsvertrages, verpflichtet sich der Auftraggeber den Auftragsverarbeiter bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten und unter Berücksichtigung des

Verschuldensgrades der Vertragsparteien zu unterstützen.

§ 7: Vertraulichkeit

Die Vertragsparteien verpflichten sich, alle Kenntnisse von betriebsinternen Geheimnissen oder datenschutzrechtlicher Sicherheitsmaßnahmen der jeweils anderen Vertragspartei vertraulich zu behandeln und nicht an Dritte weiterzugeben. Diese Verpflichtung gilt auch nach Beendigung des Vertrages weiterhin.

§ 8: Schriftlichkeit bei Änderungen

Jegliche Änderungen oder Ergänzungen dieser Vereinbarung bedürfen für Ihre Wirksamkeit der Schriftform. Dies gilt auch für Änderungen dieser Schriftformklausel.

§ 9: Haftung

9.1. : Etwaige im Hauptvertrag geregelten Haftungsprivilegierungen finden auf diese Vereinbarung keine Anwendung. Für nachteilige Folgen von Verletzungen datenschutzrechtlicher Pflichten im Rahmen des vertraglich und gesetzlich bestimmten eigenen Verantwortungsbereichs haftet jede Vertragspartei im Innenverhältnis allein und uneingeschränkt. In diesem Zusammenhang verpflichten sich sowohl der Verantwortliche als auch der Auftragsverarbeiter den jeweils anderen bei einer Inanspruchnahme durch Dritte vollumfänglich schad- und klaglos zu halten.

Davon sind insbesondere auch behördliche Geldbußen umfasst, die über eine Vertragspartei aufgrund des der anderen Vertragspartei zuzurechnenden Verhaltens verhängt wurden.

9.2. : Die Vergütung des Auftragsverarbeiters ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Auftragsverarbeitungsvertrages erfolgt nicht.

§ 10: Weisungsbefugnis & Wahrung des Berufsgeheimnisses

10.1. : Der Auftragsverarbeiter darf personenbezogene Daten nur im Rahmen des Hauptvertrages sowie der Weisungen des Auftraggebers verarbeiten und nur insoweit die Verarbeitung im Rahmen des Hauptvertrages erforderlich ist.

10.2. : Die Weisungen werden anfänglich durch den Hauptvertrag oder diesen Auftragsverarbeitungsvertrag festgelegt und können vom Auftraggeber danach durch Weisungen in schriftlicher Form oder in einem elektronischen Format (Textform, z. B. E-Mail) an den Auftragsverarbeiter oder die vom Auftragsverarbeiter bezeichnete Stelle geändert, ergänzt oder ersetzt werden.

10.3. : Mündliche Weisungen können erfolgen, wenn sie aufgrund der Umstände (z. B. Eilbedürftigkeit) geboten sind und sind unverzüglich schriftlich oder in elektronischer Form zu bestätigen.

10.4. : Ist der Auftragsverarbeiter aufgrund objektiver Umstände der Ansicht, dass eine Weisung des Auftraggebers gegen geltendes Datenschutzrecht verstößt, wird der Auftragsverarbeiter den Auftraggeber unverzüglich darauf hinweisen und die Ansicht sachlich begründen. In diesem Fall ist der Auftragsverarbeiter berechtigt, die Ausführung der Weisung bis zur ausdrücklichen Bestätigung der Weisung durch den Auftraggeber auszusetzen und offensichtlich rechtswidrige Weisungen abzulehnen.

10.5. : Der Auftragsverarbeiter kann Weisungen ablehnen, sofern deren Erfüllung dem Auftragsverarbeiter nicht möglich oder nicht zuzumuten ist (insbesondere, weil deren Befolgung ein unverhältnismäßiger Aufwand oder fehlende technische Möglichkeiten entgegenstehen). Die Ablehnung kann nur unter sachgerechter Berücksichtigung des Schutzes der Daten der betroffenen Personen erfolgen und berechtigt den Auftraggeber zur außerordentlichen Kündigung des Auftragsverarbeitungsvertrages, wenn dessen Fortsetzung dem Auftraggeber nicht zuzumuten ist.

10.6. : Der Auftragsverarbeiter kann durch das Recht der Union oder der Mitgliedstaaten und behördliche sowie gerichtliche Maßnahmen, denen der Auftragsverarbeiter unterliegt, zur Durchführung von Verarbeitungen oder Mitteilung von Informationen verpflichtet werden. In einem solchen Fall teilt der Auftragsverarbeiter dem Auftraggeber die rechtlichen Anforderungen der zwingenden gesetzlichen Verpflichtung vor der Verarbeitung mit, sofern das betreffende Gesetz oder die Anordnung eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet; im Fall eines Verbotes der Mitteilung unternimmt der Auftragsverarbeiter die ihm möglichen und zumutbaren Maßnahmen, um die gesetzlich zwingende Verarbeitung zu verhindern oder einzuschränken.

10.7. : Der Auftragsverarbeiter hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

10.8. : Der Auftragsverarbeiter benennt die zum Empfang von Weisungen berechtigte Ansprechpartner und ist verpflichtet Änderungen der Ansprechpartner oder deren Kontaktinformationen sowie Vertreter im Fall einer nicht vorübergehenden Abwesenheit oder Verhinderung unverzüglich mitzuteilen.

10.9. : Die folgenden Verpflichtungen des Abschnitts "Wahrung des Geheimnisses" dieses Auftragsverarbeitungsvertrages, kommen zur Anwendung, falls die im Auftrag verarbeiteten Daten Berufsgeheimnisse im Sinne des § 203 StGB umfassen. Die Verpflichtungen gelten unabhängig von den zeitlichen Regelungen dieses Auftragsverarbeitungsvertrages auch nach Vertragsende zeitlich unbeschränkt.

10.10. : Der Auftragsverarbeiter darf sich nur insoweit Kenntnis von Berufsgeheimnissen verschaffen, als dies für die Durchführung des Hauptvertrages sowie dieses Auftragsverarbeitungsvertrages und Erfüllung der vertraglichen Verpflichtungen erforderlich ist.

10.11. : Der Auftraggeber belehrt den Auftragsverarbeiter darüber, dass der Verstoß gegen die Vertraulichkeitsverpflichtungen entsprechend dem Gesetz und diesem Auftragsverarbeitungsvertrag durch Bruch der Verschwiegenheit oder die Verwertung fremder Geheimnisse gem. §§ 203 Abs. 1, Abs. 4 S. 1 StGB, § 204 StGB zur Bestrafung des Auftragsverarbeiters, womit auch für den Auftraggeber handelnde Personen mit umfasst

sind, mit einer Freiheitsstrafe bis zu einem Jahr, im Fall von § 204 StGB mit Freiheitsstrafe bis zu zwei Jahren, oder mit Geldstrafe bestraft werden kann. Die Strafandrohung erhöht sich auf eine Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe, sofern der Täter in Bereicherungsabsicht, auch wenn sie zu Gunsten Dritter bestehen sollte, handelt, oder die Absicht hat, durch die Tat einen anderen zu schädigen.d. Sofern der Auftragsverarbeiter Dritte (z. B. Subunternehmer) beauftragt, die an der Auftragsverarbeitung des Auftragsverarbeiters mitwirken und Kenntnis von den Berufsgeheimnissen erlangen können, verpflichtet er die Dritten entsprechend zumindest in Textform zur Verschwiegenheit. Ferner unterrichtet der Auftragsverarbeiter die Dritten über deren Pflichten. Unabhängig von der vorstehenden Verpflichtung, muss der Auftraggeber den Einsatz von Dritten erlaubt haben. Der Auftraggeber belehrt den Auftragsverarbeiter vorsorglich, dass eine Einschaltung Dritter zu einer Freiheitsstrafe von bis zu einem Jahr oder Geldstrafe führen kann, wenn ein Dritter die Verschwiegenheit bricht, und der Auftragsverarbeiter zugleich nicht dafür Sorge getragen hat, dass der Dritte zur Verschwiegenheit verpflichtet wurde (§§ 203 Abs. 1, Abs. 4 S. 2 Nr. 2 StGB). Die Strafdrohung erhöht sich auf Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe, sofern der Täter in Bereicherungsabsicht, auch wenn sie zu Gunsten Dritter bestehen sollte, handelt, oder die Absicht hat, durch die Tat einen anderen zu schädigen.

§ 11: Rechtswahl und Gerichtsstand

Diese Vereinbarung unterliegt deutschem Recht sowie dem sachlich relevanten Unionsrecht, insbesondere der DSGVO. Ausschließlicher Gerichtsstand ist der Sitz des Auftragsverarbeiters.

§ 12: Maßnahmen bei Gefährdung oder Verletzung des Datenschutzes

Die Information über eine (mögliche) Verletzung des Schutzes personenbezogener Daten hat unverzüglich, grundsätzlich innerhalb von zwei Arbeitstagen ab Kenntniserlangung zu erfolgen.

12.1. : Für den Fall, dass der Auftragsverarbeiter Tatsachen feststellt, welche die Annahme begründen, dass der Schutz der für den Auftraggeber verarbeiteten personenbezogenen Daten im Sinne des Art. 4 Nr. 12 DSGVO verletzt sein könnte, hat der Auftragsverarbeiter den Auftraggeber unverzüglich und vollständig zu informieren, unverzüglich erforderliche Schutzmaßnahmen zu ergreifen, und bei der Erfüllung der dem Auftraggeber obliegenden Pflichten, insbesondere im Zusammenhang mit der Meldung an zuständige Behörden oder betroffene Personen zu unterstützen.

12.2. : Die Meldung des Auftragsverarbeiters muss entsprechend Art. 33 Abs. 3 DSGVO, mindestens die folgenden Angaben beinhalten:

a. Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der betroffenen Kategorien von Daten und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlauf- oder Kontaktstelle für weitere Informationen;
c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten (z. B. unter Angabe weiterer Details: Identitätsdiebstahl, Vermögensnachteile, etc.);
d. eine Beschreibung der vom Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

12.3. : Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen oder von ihm Beauftragten gegen datenschutzrechtliche Bestimmungen oder die in diesem Auftragsverarbeitungsvertrag getroffenen Festlegungen.

§ 13: Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Vertrages undurchführbar oder unwirksam sein, wird die Wirksamkeit der übrigen Bestimmungen davon nicht berührt.

Anhang 1: Datenverarbeitungsspezifikationen

Bereich: Auftragsverarbeitungsvertrag

Verarbeitung	AVV
Zweck der Verarbeitung	Werbung und Marketing (Beratung, Konzeption, Umsetzung und Durchführung), IT-Dienstleistung
Personengruppe	• Mitarbeiter:innen • Kund:innen • Lieferant:innen • Dienstleister:innen
Empfänger	• sevDESK GmbH • Sendinblue GmbH - Brevo Newsletter • Microsoft Deutschland GmbH • Meta Platforms, Inc.

Anhang 2: Technisch organisatorische Maßnahmen (Art 32 Abs 1 DSGVO)

Schutzart: 1.1.1 Vertraulichkeit: Zutrittskontrolle
1.1.1.08 Es ist sichergestellt, dass Personen nur dort Zutritt erhalten, wo Sie für die Erfüllung Ihrer Aufgaben auch Zutritt benötigen
1.1.1.10 Besucher:innen oder Personal von Fremdfirmen müssen sich beim Zutritt in eine Besucherliste eintragen oder werden vom Empfang in eine solche eingetragen
1.1.1.11 Besucher:innen oder Personal von Fremdfirmen werden beim Verlassen des Unternehmens aus Besucherlisten ausgetragen (Zeitpunkt)
1.1.1.12 Besucher:innen oder Personal von Fremdfirmen sind verpflichtet, Besucherausweise sichtbar zu tragen
1.1.1.14 Besucher:innen oder Personal von Fremdfirmen werden von Mitarbeiter:innen begleitet

Schutzart: 1.1.2 Vertraulichkeit: Zutrittskontrolle (sensible Räume)
1.1.2.05 Bildschirme auf denen Personaldaten verarbeitet werden sind von außen (Fenster) oder innen (Glastüre oder Glasfront) nicht einsehbar
1.1.2.10 Bildschirme, auf denen sensible Kundendaten verarbeitet werden, sind von außen (Fenster) oder innen (Glastüre oder Glasfront) nicht einsehbar
1.1.2.15 In sensiblen Räumlichkeiten (Personal, Kundenverwaltung, IT) befinden sich keine Geräte, zu denen ein Benutzerkreis außerhalb der eigentlich Berechtigten Zugang benötigt (zB. Drucker)

Schutzart: 1.2 Vertraulichkeit: Zugangskontrolle
1.2.02 Laptops oder Smart Devices (Ipad etc.) werden nach Dienstende versperrt aufbewahrt oder werden mit nach Hause genommen
1.2.05 Die Anmeldung an einem Client erfolgt durch personenbezogene Benutzeraccounts (Benutzername und Passwort oder ähnliche Verfahren (Gesichtserkennung, Fingerprint etc.))
1.2.07 Sammelaccounts oder unpersonalisierte Benutzerzugänge auf Clients (mehrere Benutzer teilen sich einen Zugang) existieren nicht
1.2.08 Auf jedem verwendeten Client (Rechner) ist eine Firewall aktiv
1.2.09 Auf jedem Client Rechner ist eine Antiviren Software installiert, diese wird täglich bzw. bei einer Neuanmeldung aktualisiert
1.2.10 Eingehende Mails werden online am E-Mail Server (beim Hoster) auf Viren geprüft
1.2.11 Eingehende Mails werden online am Mail Server (Hoster) auf Spam geprüft
1.2.13 Bei Routern ins Internet (WLAN Router) sind nur die absolut erforderlichen Ports freigeschaltet
1.2.14 Der Zugang zum internen Netzwerk (WLAN) ist mit einem eigenen Passwort gesichert
1.2.16 Der Zugang zur Konfigurationsoberfläche des (WLAN) Routers wurde mit einem eigenen Benutzernamen und einem eigenen Passwort (ungleich Standard Benutzeraccount) gesichert
1.2.19 Eine Firewall ist auf jedem Übergang zum Internet aktiviert (Router)
1.2.21 Auf jedem Server und sonstigen Systemen bei denen ein Datenaustausch über das Internet erfolgt ist eine Antiviren Software installiert die täglich aktualisiert wird
1.2.24 Bei Bildschirmen die in Räumlichkeiten eingesetzt werden, zu denen Kund:innen (Patienten:innen...) Zugang haben und personenbezogene Daten verarbeitet werden, wird darauf geachtet, dass der Bildschirm nicht eingesehen werden kann. Allenfalls existiert ein entsprechender Sichtschutz.
1.2.25 Bildschirme werden automatisch bei Inaktivität gesperrt und können nur durch Eingabe des Benutzerpasswortes oder ähnliche Verfahren (Fingerprint, Gesichtserkennung, etc.) wieder entsperrt werden

Schutzart: 1.3 Vertraulichkeit: Zugriffskontrolle

1.3.01 Die Anzahl der Administratoren für Server und zentrale Software ist auf das „Notwendigste“ reduziert

1.3.02 Jeder Administrator verfügt über einen eigenen Benutzeraccount und das Passwort besteht zumindest aus 12 Stellen

1.3.06 Die Verwaltung von Benutzerrechten für genutzte Software erfolgt zentral über festgelegte Systemadministratoren

1.3.07 Jeder User erhält für jedes System und jede Software die er für seine Tätigkeit benötigt einen eigenen Benutzeraccount (keine Sammelaccounts)

1.3.08 Jeder User erhält auf Basis des "need to know" Prinzip, nur die Zugriffsrechte (auf Daten, Systeme, Software, Dateiablagesysteme) die er für seine Tätigkeit auch zwingend benötigt

1.3.09 Beim Ausscheiden von Mitarbeiter:innen aus dem Unternehmen ist sichergestellt, dass Zugriffsberechtigungen umgehend entfernt und User in Systemen nach Ablauf einer gewissen Frist auch gelöscht werden.

1.3.11 Fällt die Notwendigkeit eines oder mehrerer Zugriffsrechte bei einem Benutzer weg, dann werden ihm die Rechte auch zeitnah entzogen

Schutzart: 1.4 Vertraulichkeit: Trennungsgebot

1.4.02 Bei Softwareapplikationen die personenbezogene Daten verarbeiten existiert eine Trennung in Test- und Produktivsystem

1.4.03 Der Zugriff auf Daten in Datenbanken ist geregelt

1.4.04 Die Sicherung der Daten (Backup) erfolgt auf physisch und örtlich getrennte Medien

1.4.05 Softwareapplikationen und Dateiablagen auf die mehrere Benutzer:innen Zugriff haben, sind mit einem Berechtigungssystem ausgestattet.

1.4.06 Die Verarbeitung von personenbezogenen Daten erfolgt nur zu den festgelegten Zwecken

1.4.07 Die Weitergabe von personenbezogenen Daten erfolgt nur zu den festgelegten Zwecken

Schutzart: 1.5 Vertraulichkeit: Pseudoanonymisierung und Anonymisierung

1.5.01 Personenbezogene Daten werden so abgelegt oder gespeichert, dass die Zuordnung einer identifizierbaren Person nur auf Basis von entsprechenden Zugriffsrechten möglich ist

1.5.03 Personenbezogenen Identifikationsdaten werden maskiert und mit fixen "Dummy" Werten überschrieben

1.5.05 Pseudonyme werden natürlich auch vom ursprünglichen Verarbeiter vergeben, wie dies beispielsweise bei der IP-Adress-Vergabe durch einen Internet-Provider erfolgt..

1.5.10 Personenbezogenen Identifikationsdaten werden maskiert und mit fixen "Dummy" Werten überschrieben oder gelöscht, sobald der Zweck der Verarbeitung verloren gegangen ist.

1.5.12 Personenbezogenen Identifikationsdaten werden mit modernen kryptografischen Methoden verschlüsselt und verschlüsselt gespeichert

Schutzart: 1.6 Vertraulichkeit: Verschlüsselung

1.6.01 Festplatten in Servern werden verschlüsselt

1.6.04 Zur Datenweitergabe werden verschlüsselte Verbindungen wie https (Webseite) oder sftp (FTP Server) genutzt

1.6.06 Es wird die aktuellste Version des TLS Verschlüsselungsprotokolls verwendet

1.6.07 Die Versendung von Mails mit sensiblem Inhalt oder sensiblen Daten im Mail oder in Anhängen erfolgt verschlüsselt

1.6.08 Datenbanken in den personenbezogene Daten verarbeitet werden sind verschlüsselt

1.6.10 Verschlüsselte Datenfelder werden in Benutzeroberflächen nur berechtigten Personen entschlüsselt angezeigt. Eine Bearbeitung von verschlüsselten Feldern ist für nicht berechtigte Personen nicht möglich.

Schutzart: 2.1 Integrität: 1. Eingabekontrolle

2.1.05 Die An- und Abmeldung an Softwareapplikationen auf die mehrere Benutzer Zugriff haben wird protokolliert

2.1.06 Die An- und Abmeldung auf Servern wird protokolliert

Schutzart: 2.2. Integrität: 2. Weitergabekontrolle

2.2.01 Die Übermittlung von personenbezogenen Daten zu Lieferanten (Auftragsverarbeiter) erfolgt verschlüsselt (Mailverschlüsselung, VPN Tunnel etc.)

2.2.02 Dokumente (zB. Bestellungen) werden mit einer elektronischen Signatur gezeichnet

2.2.03 Auf Rechner wird mittels Fernwartung nur nach Zustimmung des Benutzers zugegriffen. Ausgenommen davon sind Update- und Konfigurationsvorgänge am Rechner mit Hilfe automatischer Installationstools.

2.2.04 05 Die Daten auf Datenträgern von Laptops oder Desktop-Computern werden vor deren internen oder externen Weitergabe gelöscht oder formatiert.

2.2.05 Daten auf sonstigen Datenträgern (USB Sticks, mobile Festplatten, ausgebaute Festplatten) werden vor deren internen oder externen Weitergabe gelöscht oder formatiert.

2.2.06 Bei Druckern oder Faxgeräten werden deren interne Datenträger vor der externen Weitergabe formatiert oder die Daten nach Vorgaben des Herstellers gelöscht

2.2.07 Die Weitergabe von personenbezogenen Daten an Dritte erfolgt in anonymisierter oder pseudonymisierter Form

2.2.08 Für die Aktenvernichtung werden Dienstleister (nach Möglichkeit mit Datenschutz-Gütesiegel) eingesetzt

Schutzart: 3.1 Verfügbarkeit und Belastbarkeit: Verfügbarkeitskontrolle

3.1.01 Auf Clients und Servern werden Updates und Sicherheitspatches regelmäßig eingespielt

3.1.02 Von relevanten Systemen (zB. Buchhaltung, CRM, HR Software) oder sonstigen Systemen die personenbezogene Daten verarbeitet werden, werden regelmäßige Datensicherungen erstellt

3.1.03 Datensicherungen werden räumlich getrennt von den Produktivdaten aufbewahrt

3.1.04 Es wird regelmäßig geprüft ob Datensicherungen vollständig rückgesichert werden können und Daten damit wieder hergestellt werden können

3.1.05 Datensicherungen werden nach einem definierten Zeitraum gelöscht

Schutzart: 4.1 Verfahren zur Überprüfung: Datenschutz-Management
4.1.02 Es wird ein Verzeichnis der Verarbeitungstätigkeiten geführt und laufend aktualisiert
4.1.03 Eine Überprüfung der Wirksamkeit der technisch organisatorischen Maßnahmen findet jährlich statt
4.1.04 Es existieren Abläufe zur Erfüllung der Rechte von betroffenen Personen
4.1.05 Eine Datenschutz Management Software ist im Einsatz
4.1.06 Die Informationspflichten (Datenschutzerklärung) werden regelmäßig geprüft
4.1.07 Es existiert ein Löschkonzept in dem festgelegt ist, wann, welche Daten zu löschen sind. Die Löschung von Daten wird stichprobenartig oder regelmäßig überprüft.
4.1.10 Alle Mitarbeiter:innen sind auf Vertraulichkeit und Datengeheimnis verpflichtet
4.1.11 Mitarbeiter:innen werden jährlich im Bereich Datenschutz geschult bzw. nachweislich sensibilisiert
4.1.14 Eine Richtlinie zur richtigen Verwendung und Aktualisierung von Passwörtern wurde erstellt und die Mitarbeiter werden dahingehend geschult
4.1.15 in Bereichen in denen sensible personenbezogene Daten verarbeitet werden existiert eine Clean/ Clear Desk Richtlinie. Die betroffenen Mitarbeiter werden regelmäßig dahingehend sensibilisiert.
4.1.16 Eine Clear Screen Richtlinie ist definiert und die Mitarbeiter werden regelmäßig sensibilisiert
4.1.20 Mitarbeiter:innen sind angewiesen, die gültigen Datenschutzmaßnahmen auch im Home Office zu gewährleisten

Schutzart: 4.2 Verfahren zur Überprüfung: Incident-Response-Management
4.2.02 Ein Ablauf zur Meldung von Sicherheitsverletzungen an die Datenschutz Behörde und betroffene Personen existiert
4.2.06 Zu jeder Sicherheitsverletzung werden Maßnahmen diskutiert und umgesetzt die zu einer Vermeidung oder Milderung weiterer Sicherheitsverletzungen führen (TOMs!)
4.2.07 Verarbeitungen werden hinsichtlich einer Datenschutz Folgeabschätzung geprüft. Eine solche wird bei Bedarf auch durchgeführt und dokumentiert

Schutzart: 4.4 Verfahren zur Überprüfung: Auftragskontrolle
4.4.02 Die Auswahl von Auftragnehmern erfolgt unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
4.4.04 Mit all unseren Auftragsverarbeitern haben wir einen Auftragsverarbeitervertrag abgeschlossen
4.4.05 Es sind wirksame Kontrollrechte gegenüber dem Auftragnehmern vertraglich (Auftragsverarbeitervertrag) vereinbart
4.4.06 In den Auftragsverarbeiter-Verträgen ist sicher gestellt, dass Daten nach Beendigung des Auftrags auch vernichtet oder übergeben werden
4.4.10 Mitarbeiter von Auftragnehmern werden auf das Datengeheimnis verpflichtet bzw. der Auftragnehmer muss dies seinerseits sicher stellen

Anhang 3: Subunternehmen (weitere Auftragsverarbeiter)

Bezeichnung	Land	Übermittlung Drittland
sevDESK GmbH	Deutschland	EU
Sendinblue GmbH - Brevo Newsletter	Deutschland	EU
Microsoft Deutschland GmbH	Deutschland	EU
Meta Platforms, Inc.	Ireland/ USA	Drittland