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.

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 Anhang und der eigenen Datenschutzerklärung zu entnehmen.

2.3. : 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 ausdrücklichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die Voraussetzungen gem. Art. 44 ff. DS-GVO erfüllt sind."

§ 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 Auftragsverarbeiter ist verpflichtet dem Verantwortlichen 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. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

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. Sollten die Parteien im Falle eines Einspruchs des Auftraggebers zu keiner einvernehmlichen Lösung finden können, steht dem Auftraggeber ein Sonderkündigungsrecht zu, welches auch den Dienstleistungsvertrag umfasst

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. Eine Unterbeauftragung ist nur innerhalb der EU / des EWR oder in Drittländern mit entsprechenden Datenschutzniveau erlaubt. Bei Erbringung der Leistung außerhalb der EU / des EWR stellt der Auftragsverarbeiter die Zulässigkeit der Verarbeitung durch entsprechende Maßnahmen unter Berücksichtigung der Art. 44 ff. DS-GVO sicher

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. Ein Protokoll der Löschung ist auf Anforderung des Auftraggebers vorzulegen

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 Verletzungen des Schutzes personenbezogener Daten kommt, 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 Auftragsverarbeiter hat schriftliche einen Datenschutzbeauftragten benannt, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragsverarbeiters leicht zugänglich hinterlegt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

5.14. : Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich 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 Auftragsverarbeiter ermittelt.
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 Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.
Der Auftragsverarbeiter 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.
Der Auftragsverarbeiter verpflichtet sich der Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 5.11 dieses Vertrages.

§ 6: 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.

§ 7: Schriftlichkeit bei Änderungen

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

§ 8: Haftung

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: Rechtswahl und Gerichtsstand

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

§ 10: 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 und Datenarten	AVV - E-Mailadressen und Telefon-/Handynummern von suchenden Kandidaten - Speicherung/ Verarbeitung der Suchbedürfnisse aus dem „Suchassistenten“ - Bookmarks, Beratungsanfragen, erfolgte Bewerbungen (inkl. übersendeter Daten – diese ausschließlich für den Kunden zur Verarbeitung der Bewerbung)
Zweck der Verarbeitung	- IT-Dienstleistungen - Werbung und Marketing (Beratung, Konzeption, Umsetzung und Durchführung). - Gewinnung und Verwaltung von Bewerbungen, sowie Verwaltung von Stellenanzeigen inklusive Kontaktvernetzung.
Personengruppe	- Kunden - Lieferanten - Dienstleister - Mitarbeitende - Kandidaten/ Bewerber
Empfänger	- sevDESK GmbH - Sendinblue GmbH: Brevo Newsletter - Microsoft Deutschland GmbH - AWS (Plattformhost)

Erläuterungen und Verweise zu den Empfängern:

- **sevDesk:** Online-Software für Rechnungsstellung, Buchhaltung, Banking und Steuereinreichung mit Belegspeicherung; **Dienstanbieter:** sevDesk GmbH, Hauptstraße 115, 77652 Offenburg, Deutschland; **Website:** https://sevdesk.de/; **Datenschutzerklärung:** https://sevdesk.de/sicherheit-datenschutz/. **Auftragsverarbeitungsvertrag:** https://sevdesk.de/sicherheit-datenschutz/.
- **Amazon Web Services (AWS):** Leistungen auf dem Gebiet der Bereitstellung von informationstechnischer Infrastruktur und verbundenen Dienstleistungen (z.B. Speicherplatz und/oder Rechenkapazitäten); **Dienstanbieter:** Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855, Luxemburg; **Website:** https://aws.amazon.com/de/; **Datenschutzerklärung:** https://aws.amazon.com/de/privacy/; **Auftragsverarbeitungsvertrag:** https://aws.amazon.com/de/compliance/gdpr-center/. **Grundlage Drittlandübermittlung:** EU-US Data Privacy Framework (DPF), Standardvertragsklauseln (https://aws.amazon.com/service-terms/).
- **Brevo:** E-Mail-Versand- und Automatisierungsdienste; **Dienstanbieter:** Sendinblue GmbH, Köpenicker Str. 126, 10179 Berlin, Deutschland; **Website:** https://www.brevo.com/; **Datenschutzerklärung:** https://www.brevo.com/legal/privacypolicy/. **Auftragsverarbeitungsvertrag:** https://www.sendinblue.com/wp-content/uploads/2020/04/AV_de_02_03_2020.pdf
- **Microsoft Deutschland GmbH** Anbieter für Officepaket- und Onlinekommunikationsysyteme; **Dienstanbieter:** Microsoft Deutschland GmbH, Walter-Gropius-Straße 5, 80807 München, Deutschland; **Website:** https://www.microsoft.com/de-de/; **Datenschutzerklärung:** https://www.microsoft.com/de-de/privacy/privacystatement.

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

Schutzart: 1.1.1 Vertraulichkeit: Zutrittskontrolle

Bezeichnung	Letztes Audit
1.1.1.08 Es ist sichergestellt, dass Personen nur dort Zutritt erhalten, wo Sie für die Erfüllung Ihrer Aufgaben auch Zutritt benötigen	10.06.2024
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	10.06.2024
1.1.1.11 Besucher:innen oder Personal von Fremdfirmen werden beim Verlassen des Unternehmens aus Besucherlisten ausgetragen (Zeitpunkt)	10.06.2024
1.1.1.12 Besucher:innen oder Personal von Fremdfirmen sind verpflichtet, Besucherausweise sichtbar zu tragen	10.06.2024
1.1.1.14 Besucher:innen oder Personal von Fremdfirmen werden von Mitarbeiter:innen begleitet	10.06.2024

Schutzart: 1.1.2 Vertraulichkeit: Zutrittskontrolle (sensible Räume)

Bezeichnung	Letztes Audit
1.1.2.05 Bildschirme auf denen Personaldaten verarbeitet werden sind von außen (Fenster) oder innen (Glastüre oder Glasfront) nicht einsehbar	10.06.2024
1.1.2.10 Bildschirme, auf denen sensible Kundendaten verarbeitet werden, sind von außen (Fenster) oder innen (Glastüre oder Glasfront) nicht einsehbar	10.06.2024
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)	10.06.2024

Schutzart: 1.2 Vertraulichkeit: Zugangskontrolle

Bezeichnung	Letztes Audit
1.2.02 Laptops oder Smart Devices (Ipad etc.) werden nach Dienstende versperrt aufbewahrt oder werden mit nach Hause genommen	10.06.2024
1.2.05 Die Anmeldung an einem Client erfolgt durch personenbezogene Benutzeraccounts (Benutzername und Passwort oder ähnliche Verfahren (Gesichtserkennung, Fingerprint etc.))	10.06.2024
1.2.07 Sammelaccounts oder unpersonalisierte Benutzerzugänge auf Clients (mehrere Benutzer teilen sich einen Zugang) existieren nicht	10.06.2024
1.2.08 Auf jedem verwendeten Client (Rechner) ist eine Firewall aktiv	10.06.2024
1.2.09 Auf jedem Client Rechner ist eine Antiviren Software installiert, diese wird täglich bzw. bei einer Neuanmeldung aktualisiert	10.06.2024
1.2.10 Eingehende Mails werden online am E-Mail Server (beim Hoster) auf Viren geprüft	10.06.2024
1.2.11 Eingehende Mails werden online am Mail Server (Hoster) auf Spam geprüft	10.06.2024
1.2.13 Bei Routern ins Internet (WLAN Router) sind nur die absolut erforderlichen Ports freigeschaltet	10.06.2024
1.2.14 Der Zugang zum internen Netzwerk (WLAN) ist mit einem eigenen Passwort gesichert	10.06.2024
1.2.16 Der Zugang zur Konfigurationsoberfläche des (WLAN) Routers wurde mit einem eigenen Benutzernamen und einem eigenen Passwort (ungleich Standard Benutzeraccount) gesichert	10.06.2024
1.2.19 Eine Firewall ist auf jedem Übergang zum Internet aktiviert (Router)	10.06.2024
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	10.06.2024
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.	10.06.2024
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	10.06.2024

Schutzart: 1.3 Vertraulichkeit: Zugriffskontrolle

Bezeichnung	Letztes Audit
1.3.01 Die Anzahl der Administratoren für Server und zentrale Software ist auf das „Notwendigste“ reduziert	10.06.2024
1.3.02 Jeder Administrator verfügt über einen eigenen Benutzeraccount und das Passwort besteht zumindest aus 12 Stellen	10.06.2024
1.3.06 Die Verwaltung von Benutzerrechten für genutzte Software erfolgt zentral über festgelegte Systemadministratoren	10.06.2024
1.3.07 Jeder User erhält für jedes System und jede Software die er für seine Tätigkeit benötigt einen eigenen Benutzeraccount (keine Sammelaccounts)	10.06.2024
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	10.06.2024
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.	10.06.2024
1.3.11 Fällt die Notwendigkeit eines oder mehrerer Zugriffsrechte bei einem Benutzer weg, dann werden ihm die Rechte auch zeitnah entzogen	10.06.2024

Schutzart: 1.4 Vertraulichkeit: Trennungsgebot

Bezeichnung	Letztes Audit
1.4.02 Bei Softwareapplikationen die personenbezogene Daten verarbeiten existiert eine Trennung in Test- und Produktivsystem	10.06.2024
1.4.03 Der Zugriff auf Daten in Datenbanken ist geregelt	10.06.2024
1.4.04 Die Sicherung der Daten (Backup) erfolgt auf physisch und örtlich getrennte Medien	10.06.2024
1.4.05 Softwareapplikationen und Dateiablagen auf die mehrere Benutzer:innen Zugriff haben, sind mit einem Berechtigungssystem ausgestattet.	10.06.2024
1.4.06 Die Verarbeitung von personenbezogenen Daten erfolgt nur zu den festgelegten Zwecken	10.06.2024
1.4.07 Die Weitergabe von personenbezogenen Daten erfolgt nur zu den festgelegten Zwecken	10.06.2024

Schutzart: 1.5 Vertraulichkeit: Pseudoanonymisierung und Anonymisierung

Bezeichnung	Letztes Audit
1.5.01 Personenbezogene Daten werden so abgelegt oder gespeichert, dass die Zuordnung einer identifizierbaren Person nur auf Basis von entsprechenden Zugriffsrechten möglich ist	10.06.2024
1.5.03 Personenbezogenen Identifikationsdaten werden maskiert und mit fixen "Dummy" Werten überschrieben	10.06.2024
1.5.05 Pseudonyme werden natürlich auch vom ursprünglichen Verarbeiter vergeben, wie dies beispielsweise bei der IP-Adress-Vergabe durch einen Internet-Provider erfolgt..	10.06.2024
1.5.10 Personenbezogenen Identifikationsdaten werden maskiert und mit fixen "Dummy" Werten überschrieben oder gelöscht, sobald der Zweck der Verarbeitung verloren gegangen ist.	10.06.2024
1.5.12 Personenbezogenen Identifikationsdaten werden mit modernen kryptografischen Methoden verschlüsselt und verschlüsselt gespeichert	10.06.2024

Schutzart: 1.6 Vertraulichkeit: Verschlüsselung

Bezeichnung	Letztes Audit
1.6.01 Festplatten in Servern werden verschlüsselt	10.06.2024
1.6.04 Zur Datenweitergabe werden verschlüsselte Verbindungen wie https (Webseite) oder sftp (FTP Server) genutzt	10.06.2024
1.6.06 Es wird die aktuellste Version des TLS Verschlüsselungsprotokolls verwendet	10.06.2024
1.6.07 Die Versendung von Mails mit sensiblem Inhalt oder sensiblen Daten im Mail oder in Anhängen erfolgt verschlüsselt	10.06.2024
1.6.08 Datenbanken in den personenbezogene Daten verarbeitet werden sind verschlüsselt	10.06.2024
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.	10.06.2024

Schutzart: 2.1 Integrität: 1. Eingabekontrolle

Bezeichnung	Letztes Audit
2.1.05 Die An- und Abmeldung an Softwareapplikationen auf die mehrere Benutzer Zugriff haben wird protokolliert	10.06.2024
2.1.06 Die An- und Abmeldung auf Servern wird protokolliert	10.06.2024

Schutzart: 2.2. Integrität: 2. Weitergabekontrolle

Bezeichnung	Letztes Audit
2.2.01 Die Übermittlung von personenbezogenen Daten zu Lieferanten (Auftragsverarbeiter) erfolgt verschlüsselt (Mailverschlüsselung, VPN Tunnel etc.)	10.06.2024
2.2.02 Dokumente (zB. Bestellungen) werden mit einer elektronischen Signatur gezeichnet	10.06.2024
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.	10.06.2024
2.2.04 05 Die Daten auf Datenträgern von Laptops oder Desktop-Computern werden vor deren internen oder externen Weitergabe gelöscht oder formatiert.	10.06.2024
2.2.05 Daten auf sonstigen Datenträgern (USB Sticks, mobile Festplatten, ausgebaute Festplatten) werden vor deren internen oder externen Weitergabe gelöscht oder formatiert.	10.06.2024
2.2.06 Bei Druckern oder Faxgeräten werden deren interne Datenträger vor der externen Weitergabe formatiert oder die Daten nach Vorgaben des Herstellers gelöscht	10.06.2024
2.2.07 Die Weitergabe von personenbezogenen Daten an Dritte erfolgt in anonymisierter oder pseudonymisierter Form	10.06.2024
2.2.08 Für die Aktenvernichtung werden Dienstleister (nach Möglichkeit mit Datenschutz-Gütesiegel) eingesetzt	10.06.2024

Schutzart: 3.1 Verfügbarkeit und Belastbarkeit: Verfügbarkeitskontrolle

Bezeichnung	Letztes Audit
3.1.01 Auf Clients und Servern werden Updates und Sicherheitspatches regelmäßig eingespielt	10.06.2024
3.1.02 Von relevanten Systemen (zB. Buchhaltung, CRM, HR Software) oder sonstigen Systemen die personenbezogene Daten verarbeitet werden, werden regelmäßige Datensicherungen erstellt	10.06.2024
3.1.03 Datensicherungen werden räumlich getrennt von den Produktivdaten aufbewahrt	10.06.2024
3.1.04 Es wird regelmäßig geprüft ob Datensicherungen vollständig rückgesichert werden können und Daten damit wieder hergestellt werden können	10.06.2024
3.1.05 Datensicherungen werden nach einem definierten Zeitraum gelöscht	10.06.2024

Schutzart: 4.1 Verfahren zur Überprüfung: Datenschutz-Management

Bezeichnung	Letztes Audit
4.1.02 Es wird ein Verzeichnis der Verarbeitungstätigkeiten geführt und laufend aktualisiert	10.06.2024
4.1.03 Eine Überprüfung der Wirksamkeit der technisch organisatorischen Maßnahmen findet jährlich statt	10.06.2024
4.1.04 Es existieren Abläufe zur Erfüllung der Rechte von betroffenen Personen	10.06.2024
4.1.05 Eine Datenschutz Management Software ist im Einsatz	10.06.2024
4.1.06 Die Informationspflichten (Datenschutzerklärung) werden regelmäßig geprüft	10.06.2024
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.	10.06.2024
4.1.10 Alle Mitarbeiter:innen sind auf Vertraulichkeit und Datengeheimnis verpflichtet	10.06.2024
4.1.11 Mitarbeiter:innen werden jährlich im Bereich Datenschutz geschult bzw. nachweislich sensibilisiert	10.06.2024
4.1.14 Eine Richtlinie zur richtigen Verwendung und Aktualisierung von Passwörtern wurde erstellt und die Mitarbeiter werden dahingehend geschult	10.06.2024
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.	10.06.2024
4.1.16 Eine Clear Screen Richtlinie ist definiert und die Mitarbeiter werden regelmäßig sensibilisiert	10.06.2024
4.1.20 Mitarbeiter:innen sind angewiesen, die gültigen Datenschutzmaßnahmen auch im Home Office zu gewährleisten	10.06.2024

Schutzart: 4.2 Verfahren zur Überprüfung: Incident-Response-Management

Bezeichnung	Letztes Audit
4.2.02 Ein Ablauf zur Meldung von Sicherheitsverletzungen an die Datenschutz Behörde und betroffene Personen existiert	10.06.2024
4.2.06 Zu jeder Sicherheitsverletzung werden Maßnahmen diskutiert und umgesetzt die zu einer Vermeidung oder Milderung weiterer Sicherheitsverletzungen führen (TOMs!)	10.06.2024
4.2.07 Verarbeitungen werden hinsichtlich einer Datenschutz Folgeabschätzung geprüft. Eine solche wird bei Bedarf auch durchgeführt und dokumentiert	10.06.2024

Schutzart: 4.4 Verfahren zur Überprüfung: Auftragskontrolle

Bezeichnung	Letztes Audit
4.4.02 Die Auswahl von Auftragnehmern erfolgt unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)	10.06.2024
4.4.04 Mit all unseren Auftragsverarbeitern haben wir einen Auftragsverarbeitervertrag abgeschlossen	10.06.2024
4.4.05 Es sind wirksame Kontrollrechte gegenüber dem Auftragnehmern vertraglich (Auftragsverarbeitervertrag) vereinbart	10.06.2024
4.4.06 In den Auftragsverarbeiter-Verträgen ist sicher gestellt, dass Daten nach Beendigung des Auftrags auch vernichtet oder übergeben werden	10.06.2024
4.4.10 Mitarbeiter von Auftragnehmern werden auf das Datengeheimnis verpflichtet bzw. der Auftragnehmer muss dies seinerseits sicher stellen	10.06.2024