Vertrag über die Auftragsverarbeitung personenbezogener Daten in wiredminds leadlab nach DSGVO

Ihr Team der wiredminds GmbH

Telefon: 0049 711 585 331 0
E-Mail: datenschutz@wiredminds.de
Web: www.wiredminds.de

Vertragspartner

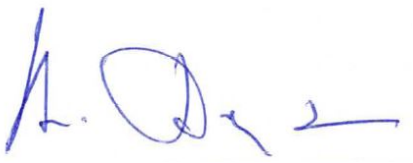
Auftragnehmer

wiredminds GmbH

Lindenspürstr. 32

70176 Stuttgart

Vertreten durch:



Albert Denz
Geschäftsführer

Auftraggeber **(bitte Daten eintragen)**

Vertreten durch: **(Bitte Daten eintragen)**

Ort, Datum

1 Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag regelt die Rechte und Pflichten von Aufraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.

(2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

(3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

(4) Sie bestätigen mit Ihrer Unterschrift, dass Sie diesen „Vertrag über die Auftragsverarbeitung personenbezogener Daten in wiredminds leadlab nach DSGVO“ ohne Anpassungen (Ausnahme Punkt 2) anerkennen.

2 Gegenstand und Dauer der Verarbeitung

2.1. Gegenstand
Gegenstand, Art und Umfang sowie Zweck der Datenverarbeitung ergeben sich aus dem zwischen der Dateninhaberin und dem Vertragspartner geschlossenen Hauptvertrag:

Bezeichnung des Hauptvertrages: _____

Datum des Vertragsabschlusses: _____

2.2. Dauer
Die Verarbeitung beginnt am

Datum des Projektstarts: _____

und erfolgt auf unbestimmte Zeit bis zur Beendigung (Punkt 11) dieses Vertrags oder des Hauptvertrags durch eine Partei.

3 Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:

3.1. Art und Zweck der Verwendung
Die Verarbeitung ist folgender Art:

Erheben, Erfassen, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Bereitstellung, Abgleich, Einschränkung, Löschen oder Vernichtung von Daten

Die Verarbeitung dient folgendem Zweck:

wiredminds leadlab erfasst die Besuchsdaten der Domain des Auftraggebers und wertet die Daten von identifizierten Firmenbesuchen aus. Dabei wird das Nutzungsverhalten analysiert um einen möglichen Interessenschwerpunkt des Besuchers zu erkennen.

Die erfassten Daten werden dem Auftraggeber in einer cloudbasierten Softwarelösung zugänglich gemacht. Zusätzlich haben einzelne Mitarbeiter von wiredminds Zugriff auf diese Daten um Themen aus dem Bereich Support, Wartung, Entwicklung umsetzen zu können. Gespeichert werden die Daten darüber hinaus bei unserem Hosting Partner. Hier bestehen aber keine Zugriffsrechte auf die Daten durch die Mitarbeiter unseres Hosting-Partners.

3.2. Art der Daten
Bei der Verwendung der Software werden unter anderem folgende Arten von Daten erhoben:

- Benutzerkennungen und Benutzerstammdaten der Mitarbeiter des Auftraggebers (Software-Nutzer)
- Benutzernutzungsdaten der Mitarbeiter des Auftraggebers in Form von Log-Dateien (Service-Monitoring und Security)
- Hosting von CRM-Daten, die auch personenbezogen sein können wie z. B. Notizen

Von den erfassten Besuchern der Webseite werden folgende Arten von Daten erhoben:

- IP-Adresse des Webseitenbesuchers
  Dabei wird die IP-Adresse nicht gespeichert. Die IP Adresse dient lediglich zur Ausfilterung natürlicher Personen um deren Schutz zu ermöglichen.

03. Kategorien der betroffenen Personen
Von der Verarbeitung betroffen sind:

- Mitarbeiter des Auftraggebers (Benutzer von leadlab)
- Besuche (juristischer Personen) der Webseite des Auftraggebers

4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind.

(3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

(4) Personen, die Kenntnis von den im Auftrag verarbeiteten personenbezogenen Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

(5) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

(6) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Die dafür erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

(7) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

(8) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

(9) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.

(10) Die Auftragsverarbeitung erfolgt ausschließlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

5 Technische und organisatorische Maßnahmen

(1) Die im Anhang 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum.

(2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Der Auftraggeber hat das Recht, einer Änderung der technisch und organisatorischen Maßnahmen innerhalb von 4 Wochen mit Begründung gegenüber dem Auftragnehmer schriftlich zu widersprechen. Erfolgt kein begründeter Widerspruch, gilt die Änderung als genehmigt.

(3) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

(4) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

(5) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

(6) Die Verarbeitung von Daten im HomeOffice ist zulässig, sofern der betreffende Mitarbeiter die aktuell gültige HomeOffice Vereinbarung mit dem Arbeitgeber (Auftragnehmer) abgeschlossen hat. Soweit eine solche Verarbeitung erfolgt, ist vom Auftragnehmer sicherzustellen, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird und die in diesem Vertrag bestimmten Kontrollrechte des Auftraggebers uneingeschränkt auch in den betroffenen Privatwohnungen ausgeübt werden können. Die Verarbeitung von Daten im Auftrag mit Privatgeräten ist unter keinen Umständen gestattet.

(7) Der Auftragnehmer führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen. Dieser Nachweis kann auf Wunsch des Auftraggebers jederzeit zur Verfügung gestellt werden. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden.

6 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

(1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.

(2) Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten, es sei denn, die Weisung sind rechtswidrig, entsprechen nicht den Regelungen dieses Vertrages oder sind tatsächlich für den Auftragnehmer unmöglich zu erfüllen.

7 Unterauftragsverhältnisse

(1) Der Auftraggeber stimmt allgemein zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Die Beauftragung von Subunternehmern, d. h. jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Subunternehmer, ist dem Auftraggeber in jedem Einzelfall schriftlich anzuzeigen. Der Auftraggeber hat das Recht, einer Subbeauftragung innerhalb von 4 Wochen mit Begründung schriftlich zu widersprechen. Erfolgt kein begründeter Widerspruch, gilt der Einsatz des Subunternehmers als genehmigt. Der Auftraggeber kann die Genehmigung jederzeit schriftlich aussprechen. Vor Genehmigung werden dem Subunternehmer keine im Auftrag verarbeiteten Daten zugänglich gemacht. Sofern eine einvernehmliche Lösung hinsichtlich der Begründung des Widerspruchs zwischen den Parteien nicht möglich ist, sind beide Parteien innerhalb von 14 Tagen zur außerordentlichen Kündigung dieses Vertrags und des Hauptvertrages berechtigt.

(2) Die Auftragsvergabe an Subunternehmer muss schriftlich erfolgen. Der Auftragnehmer hat den Subunternehmer sorgfältig auszuwählen. Er hat sich vor Beginn der Datenverarbeitung durch den Subunternehmer und sodann regelmäßig von der Einhaltung der beim Subunternehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen und die Ergebnisse zu dokumentieren. Dem Auftraggeber ist auf Verlangen eine Ausfertigung des Auftrages sowie der Prüfdokumentation zur Verfügung zu stellen.

(3) Wenn Subunternehmer durch den Auftragnehmer eingeschaltet werden, so werden die vertraglichen Vereinbarungen so gestaltet, dass sie den Anforderungen dieser Vereinbarung entsprechen. Dem Auftraggeber sind Kontroll- und Überprüfungsrechte entsprechend § 8 dieser Vereinbarung einzuräumen. Ebenso ist der Auftraggeber berechtigt, auf schriftliche Anforderung vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

(4) Sofern der Subunternehmer außerhalb eines in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum stammt oder die Datenverarbeitung dort stattfindet, ist durch den Auftragnehmer darüber hinaus sicherzustellen, dass die in Kapitel 4 (10) genannten Bedingungen beachtet werden. Dies ist dem Auftraggeber gegenüber schriftlich vor Aufnahme der Tätigkeiten des Subunternehmers nachzuweisen.

8 Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(4) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

(5) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Kapitel 5 (8) dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

9 Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle sind mitzuteilen. Die Mitteilung hat mindestens die Angaben **nach Art. 33 Abs. 3 Datenschutz-Grundverordnung** zu enthalten.

(2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

(4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

10 Weisungen

(1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

(2) Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 3.

(3) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

(4) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(5) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

11 Beendigung des Auftrags

(1) Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist. Eine physische Vernichtung erfolgt gemäß DIN 66399. Hierbei gilt mindestens Schutzklasse 3.

(2) Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

(3) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.

(4) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

12 Haftung

(1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.

(2) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.

(3) Nummer (3) gilt nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

13 Sonderkündigungsrecht

(1) Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

(2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

(3) Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

14 Sonstiges

(1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

(2) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(3) Für Nebenabreden ist die Schriftform erforderlich.

(4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

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

15 Anlagen

Anlage 1: Beschreibung der technischen-organisatorischen Maßnahmen

Anlage 2: Datenschutzbeauftragter des Auftragnehmers

Anlage 3: Weisungsgeber und Weisungsnehmer

Anlage 4: Beauftragte Subunternehmer

Anlage 1

Technische und organisatorische Maßnahmen zur Sicherheit der Datenverarbeitung

Nachstehend wird beschrieben, welche technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt sind. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Unternehmen verarbeiteten Informationen. Die Struktur orientiert sich nach der international anerkannten Norm DIN ISO/IEC 27002.

01. Leitlinie

Die Datenschutzleitlinie der wiredminds GmbH beinhaltet die Leitaussagen der Geschäftsleitung zum Umgang mit personenbezogenen Daten im Unternehmen. Alle Beschäftigten, freie Mitarbeiter und unterstützende Unternehmen sind verpflichtet diese zentralen Regelungen zu beachten. Das erreichte IT-Sicherheitsniveau der Organisationseinheiten, Prozesse und Systeme wird durch eine Kombination aus periodisch wiederkehrenden Prüfungen und kontinuierlichen Kontrollen überwacht.

Die Überwachungen des laufenden Betriebs erfolgen in Abstimmung mit dem Sicherheitsbeauftragten. Ein Review der Sicherheitspolitik erfolgt zumindest jährlich, soweit nicht eine essentielle Änderung dies früher erfordert.

Hierdurch wird die laufende Angemessenheit, Eignung und Effektivität der Regelung sicher-gestellt. Der Sicherheitsbeauftragte ist der Verantwortliche für die Sicherheitspolitik und hat die Verantwortung, diese zu entwickeln, zu überarbeiten und zu prüfen.

02. Organisation der Informationssicherheit

Die Führungskräfte der wiredminds GmbH sind in ihrer Organisationseinheit für die vollständige Umsetzung der Grundsätze der IT-Sicherheit und für die Erfüllung der an sie gestellten IT-Sicherheits-aufgaben verantwortlich.

Informationssicherheitsrollen und -verantwortlichkeiten sind in der IT-Sicherheitsorganisation definiert. Miteinander in Konflikt stehende Aufgaben und Verantwortlichkeitsbereiche sind getrennt, um die Möglichkeiten zu unbefugter oder unbeabsichtigter Änderung oder zum Missbrauch der Werte unseres Unternehmens zu reduzieren.

Wir verfügen über ein Verfahren, das festlegt, wann und durch wen relevante Behörden benachrichtigt und erkannte Datenschutz- und Informationssicherheitsvorfälle rechtzeitig gemeldet werden. Auch pflegen wir laufenden Kontakt zu speziellen Interessensgruppen, um über Änderungen und Verbesserungen im Bereich Datenschutz und Informationssicherheit informiert zu sein.

In unseren Projekten ist Datenschutz und Datensicherheit Bestandteil aller Phasen unserer Projektmethodik. Durch unsere jeweiligen Richtlinien und Prozesse zur Telearbeit und der Nutzung von Mobilgeräten, stellen wir den Datenschutz und die Datensicherheit auch in diesen Bereichen sicher.

Anlage 1

Technische und organisatorische Maßnahmen zur Sicherheit der Datenverarbeitung

03. Personalsicherheit
Wir haben unsere Mitarbeiter sorgsam ausgewählt und ihre Eignung für ihre Rolle im Unternehmen überprüft. Ihre Verantwortlichkeiten haben wir in Funktionsbeschreibungen festgelegt und gleichen regelmäßig ab, ob die Mitarbeiter diesen entsprechen. Vor Beginn ihrer Anstellung unterschreiben alle Mitarbeiter eine Vertraulichkeits- sowie Datenschutzvereinbarung, die über die Beendigung des Beschäftigungsverhältnisses hinaus gilt. Die Mitarbeiter werden im Bereich Datenschutz- und Datensicherheit geschult, insbesondere werden Schulungen bei Funktionswechsel noch einmal aufgefrischt. Sie sind sich daher ihrer Verantwortung diesbezüglich bewusst.

In einem dokumentierten Prozess für die Zeit vor, während und nach Beendigung des Beschäftigungsverhältnisses stellen wir sicher, dass personenbezogene Daten geschützt und die Datensicherheit gewährleistet ist. Diese beinhaltet auch Maßregelungen für den Fall eines Datenschutzverstoßes.

04. Verwaltung der Werte
Sämtliche Werte (wie z.B. Betriebsmittel, Notebooks, Smartphones) und Informationen, die mit personenbezogenen Daten in Zusammenhang stehen, werden von uns inventarisiert und gepflegt.

Wir haben zum Schutz dieser Werte Verantwortliche festgelegt, die für den Lebenszyklus eines Wertes zuständig sind.

Es wurden dokumentierte Regeln für den zulässigen Gebrauch unserer Werte aufgestellt. Die Rückgabe erfolgt dokumentiert.

Unsere Informationen und Daten werden anhand der gesetzlichen Anforderungen, ihres Wertes, ihrer Kritikalität und ihrer Empfindlichkeit gegenüber unbefugter Offenlegung oder Veränderung klassifiziert und gekennzeichnet.

Diesem Klassifizierungsschema entsprechend, haben wir dokumentierte Verfahren für die Handhabung unserer Werte entwickelt und umgesetzt. Wir übertragen üblicherweise Daten nicht auf Wechseldatenträgern, sondern ausschließlich in verschlüsselter Form über verifizierte Kommunikationswege. Nur auf schriftliche Weisung des Auftraggebers kann in Ausnahmefällen von dieser Praxis abgewichen werden.

Nicht mehr benötigte Datenträger entsorgen wir sicher, unter Anwendung eines dokumentierten Verfahrens und verpflichteter zertifizierter Dienstleister.

Anlage 1
Technische und organisatorische Maßnahmen zur Sicherheit der Datenverarbeitung

05. Zugriffssteuerung
Wir verfügen über geregelte und dokumentierte Maßnahmen, die sicherstellen, dass berechtigte Personen nur auf solche personenbezogenen Daten Zugriff erhalten, für die sie die Befugnis zur Einsichtnahme und zur Verarbeitung besitzen.

Berechtigungen zum Zugriff auf IT-Systeme werden über ein geregeltes Verfahren auf der Grundlage eines dokumentierten und restriktiven Berechtigungskonzepts vergeben. Den Zugang zu Netzwerken und Netzwerkdiensten haben wir geregelt und umgesetzt.

Es ist sichergestellt, dass nur befugte Benutzer Zugang zu Systemen und Diensten haben und unbefugter Zugang unterbunden wird, insbesondere besteht ein formaler Prozess für die Registrierung und der Registrierung von Benutzern, der die Zuordnung von Zugangsrechten zu ermöglicht.
Unsere administrativen Rechte erteilen wir eingeschränkt und gesteuert.

Wir verfügen über einen dokumentierten und geregelten Prozess über den Umgang mit Passwörtern.

Ist- und Soll-Zustand von Benutzerzugangsrechten werden regelmäßig abgeglichen. Bei Bedarf werden diese entzogen oder angepasst.

Wir schränken den Zugriff auf unsere Daten bedarfsgerecht ein und steuern den Zugang auf unsere Systeme und Anwendungen durch ein sicheres Anmeldeverfahren. Wir verwenden ein System zur Nutzung sicherer und starker Kennwörter.

Der Gebrauch von Hilfsprogrammen, die fähig sein könnten, System- und Anwendungsschutz-maßnahmen zu umgehen, ist eingeschränkt und streng überwacht.

06. Kryptographie
Der angemessene und wirksame Gebrauch von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Information ist sichergestellt. Zu diesem Zwecke haben wir eine Richtlinie über den Einsatz von Kryptographischen Maßnahmen im Unternehmen implementiert, die auch die Verwaltung von kryptographischen Schlüsseln umfasst und dem Schutzbedarf angemessen ist.

Anlage 1
Technische und organisatorische Maßnahmen zur Sicherheit der Datenverarbeitung

07. Physische und umgebungsbezogene Sicherheit

Wir haben dokumentierte und geregelte Maßnahmen getroffen, die verhindern sollen, dass Unbefugte Zutritt zu Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet oder genutzt werden. Diese umfassen unter anderem:

- Die Geschäftsräume liegen im 3. Stockwerk eines Bürogebäudes und werden exklusiv genutzt.
- Der zentrale Eingang wird überwacht.
- Türen zu Sicherheitsbereichen sind stets geschlossen.
- Besucher oder externe Dienstleister werden individuell eingelassen.
- Der Brandschutz wird beachtet
- Es sind Sicherheitsbereiche vorhanden, zu denen nur eigens hierzu Berechtigte Zutritt erhalten.
- IT-Räume sind separat verschlossen und nur durch Berechtigte zu öffnen.
- Versorgungseinrichtungen werden vor Stromausfällen und Störungen geschützt
- Die Sicherheit der Verkabelung wird beachtet
- Die Instandhaltung von Systemen wird geplant und umgesetzt
- Das Entfernen und Änderungen von Systemen und Informationen erfolgt geregelt.
- Die Sicherheit von Systemen außerhalb der Geschäftsräume wird beachtet.
- Die Entsorgung oder Wiederverwendung von Betriebsmitteln erfolgt geregelt
- Unbeaufsichtigte Benutzergeräte werden durch Verschlüsselung geschützt
- Richtlinien für Clean Desk und Bildschirmsperren werden umgesetzt.

Anlage 1
Technische und organisatorische Maßnahmen zur Sicherheit der Datenverarbeitung

08. Betriebssicherheit

Wir verfügen über geregelte und dokumentierte Maßnahmen, um einen ordnungsgemäßen und sicheren Betrieb von informations- und datenverarbeitenden Einrichtungen sicherzustellen. Diese umfassen u.a. die Steuerung im Falle einer Änderung an den informationsverarbeitenden Einrichtungen, als auch eine Steuerung und regelmäßige Messung unserer Kapazitäten und Ressourcen, um die Verfügbarkeit der erforderlichen Systemleistung sicherzustellen. So werden z.B. unter anderem folgende Werte laufend aktuell überwacht:

- Festplattenstatus und verfügbarer Speicher
- Raid-Status
- Dienste und Status aller virtuellen Maschinen
- Fehlerhafte Anmeldeversuche
- Speicherbelegung der Storages und Hauptspeicher
- Auslastung Ethernet in Kbit/s und Mbit/s
- Anzahl der RDP-Sessions der einzelnen Terminal-Server
- Durchsatz und Auslastung der Firewall
- Erreichbarkeit aller Server von außen
- Erreichbarkeit und Durchsatz der Switche

Ein geschütztes Verfahren zur Datensicherung wurde von uns implementiert und ist dokumentiert. Standardwartungsfenster sind definiert. Zusätzlich notwendige Fenster werden mindestens 10 Tage vorab angekündigt.

In unserem Unternehmen ist es essentiell, Entwicklungs-, Test und Betriebsumgebungen voneinander zu trennen, so dass wir ein besonderes Augenmerk hierauf haben.

Maßnahmen zur Erkennung, Vorbeugung und Wiederherstellung zum Schutz von Schadsoftware wurden getroffen und werden regelmäßig aktualisiert.

Wir verfügen über eine zentral überwachte und geschützte Ereignisprotokollierung und haben für den Fall der Speicherung sensibler personenbezogener Daten Maßnahmen zum Schutz der Privatsphäre getroffen. Sämtliche Protokollierungseinrichtungen und Protokollinformationen, einschließlich Administratoren und Bedienerprotokolle sind vor Manipulation und unbefugtem Zugriff geschützt.

Die Synchronisation unserer Uhren erfolgt zentral mit einer einzigen Referenzzeitquelle.

Wir verfügen über ein zentrales Verfahren zur gesteuerten Installation von Software auf Systemen in unserem Unternehmen.

Anlage 1
Technische und organisatorische Maßnahmen zur Sicherheit der Datenverarbeitung

Es besteht eine Aufstellung unserer technischen Werte und eine geregelte, dokumentierte Handhabung für den Fall einer technischen Schwachstelle, die u.a. unser Patchmanagement mit definierten Verantwortlichkeiten umfasst.

Regelungen für die Einschränkungen von Softwareinstallationen sind von uns zentral implementiert.

Im Falle einer Auditprüfung unserer Informationssysteme haben wir Maßnahmen festgelegt, die Störungen der Geschäftsprozesse soweit wie möglich minimieren.

09. Kommunikationssicherheit

Die Sicherheit unserer in Netzwerken und Netzwerkdiensten gespeicherten personenbezogenen Daten und Informationen ist unumgänglich. Daher haben wir dokumentierte Maßnahmen eingesetzt, die unsere Netzwerke verwalten, steuern und sichern.

Informationsdienste, Benutzer und Informationssysteme werden bedarfsgerecht voneinander getrennt gehalten.

Wir verfügen über Richtlinien und Verfahren für die Informations- und Datenübertragung, sowie die Vereinbarungen zur Informationsübertragung an externe Stellen.

Unsere elektronische Nachrichtenübermittlung wird angemessen geschützt. So haben wir unter anderem Maßnahmen zum Schutz der Nachrichten vor unbefugtem Zugriff, vor Veränderung oder Denial of Service getroffen, die dem von der Organisation übernommenen Klassifizierungsschema entsprechen.

Um unsere Daten zu schützen, schließen wir bedarfsgerechte Vertraulichkeits- oder Geheimhaltungsvereinbarungen ab, die wir regelmäßig überprüfen.

Anlage 1
Technische und organisatorische Maßnahmen zur Sicherheit der Datenverarbeitung

10. Anschaffung, Entwicklung und Instandhaltung von Systemen

Es ist sichergestellt, dass Daten- und Informationssicherheit ein fester Bestandteil über den gesamten Lebenszyklus unserer Systeme ist. Dies beinhaltet auch die Anforderungen an und die Sicherung von Informationssystemen, die Dienste über öffentliche Netze bereitstellen. Der Schutz der Transaktionen bei Anwendungsdiensten erfolgt bedarfsgerecht. Zudem haben wir ein Verfahren zur Verwaltung von Systemänderungen eingerichtet, um die Integrität des Systems, der Anwendungen und der Produkte von den frühen Entwurfsphasen bis zu allen später anfallenden Wartungsarbeiten sicherzustellen.

Bei Änderungen an Betriebsplattformen werden geschäftskritische Anwendungen überprüft und getestet, um sicherzustellen, dass es keine negativen Auswirkungen auf die Organisationssicherheit auch der Kundenanwendungen gibt. Wir verfügen über einen gesteuerten Prozess zur Analyse, der Entwicklung und der Pflege sicherer IT Systeme.

Für neue Informationssysteme, Aktualisierungen und neue Versionen sind Abnahmetestprogramme und dazugehörige Kriterien festgelegt. Unsere Testdaten werden sorgfältig ausgewählt geschützt und gesteuert.

11. Lieferantenbeziehungen

Wir wählen unsere Lieferanten im Vorfeld sorgsam aus und überprüfen ihre Geeignetheit hinsichtlich der Wahrung des Daten- und Informationssicherheitsschutzes.

Dokumentierte Vereinbarungen sichern den Schutz und die Geheimhaltung unserer Werte und Daten. Die Lieferanten werden verpflichtet, technisch-organisatorische Maßnahmen zu treffen, um dies zu gewährleisten.

Es besteht eine reglementierte und benutzerdefinierte Zugriffsberechtigung auf die für den jeweiligen Lieferanten zwingend benötigten Werte und Daten.

Lieferanten dürfen weitere Lieferanten lediglich mit unserer Zustimmung beauftragen, um eine sichere Lieferkette zu gewährleisten.

Regelmäßig führen wir eine Überprüfung der Datenschutz- und Datensicherheitsmaßnahmen unserer Lieferanten durch, um das vereinbarte Niveau aufrecht zu erhalten. Auch die zugewiesenen Berechtigungen unterliegen einer ständigen dokumentierten Kontrolle.

Nach Beendigung des Lieferantenverhältnisses sind diese verpflichtet, die von uns erhaltenen Daten und Werte zu vernichten. Zudem gilt die Wahrung der Geheimhaltungspflicht unbegrenzt.

Anlage 1
Technische und organisatorische Maßnahmen zur Sicherheit der Datenverarbeitung

12. Handhabung von Informationssicherheits- und Datenschutzereignissen

Unser Unternehmen verfügt über einen geregelten dokumentierten Prozess für die Handhabung von Informationssicherheits- und Datenschutzvorfällen, um diesbezüglich eine konsistente und wirksame Herangehensweise zu gewährleisten. Die Mitarbeiter sind angehalten, sämtliche Datenschutz – und Sicherheitsereignisse unverzüglich zu melden und werden diesbezüglich regelmäßig geschult. Wir haben ein Meldesystem installiert, das Ereignisse an ein Interventionsteam weitergeleitet, um eine schnelle Reaktion zu gewährleisten. Sämtliche Ereignisse werden dokumentiert, klassifiziert und bewertet. Das implementierte Interventionsteam hat genaue Vorgaben, wie auf ein Ereignis zu reagieren ist.

Zusammen mit der Geschäftsführung werden regelmäßig Verbesserungsmaßnahmen besprochen und umgesetzt, die sich aus den Erkenntnissen und den gesammelten Beweisen eines Ereignisses ergeben.

13. Informationssicherheitsaspekte beim Business Continuity Management

Im Rahmen der Informationssicherheit wird die vorgesehene Verfügbarkeit von Systemen eigens bewertet und dokumentiert. Aus den Anforderungen leiten wir die technischen und organisatorischen Vorgaben, wie redundante Systeme / Anbindungen oder entsprechende Planungen ab und setzen diese konsequent und gesteuert um.

Ein übergreifender Notfallplan bildet den Rahmen bezüglich der entsprechenden Handlungsanweisungen für ausgewählte dokumentierte Notfallszenarien.

Laufende aktualisierte Übungspläne für die Erprobung der eingesetzten Maßnahmen und die Dokumentation der Durchführung entsprechender Tests rundet das Notfallmanagement ab. Alle Server und Storage Systeme sind bei einem ausgewählten Rechenzentrum angemietet. Aufgrund der vertraglichen Vereinbarungen besteht ein dauerhafter Anspruch auf Verfügbarkeit gegenüber dem Dienstleister.

Anlage 1
Technische und organisatorische Maßnahmen zur Sicherheit der Datenverarbeitung

14. Compliance

Wir haben alle relevanten gesetzlichen, regulatorischen, selbstauferlegten oder vertraglichen Anforderungen sowie das Vorgehen unseres Unternehmens zur Einhaltung dieser Anforderungen bestimmt, dokumentiert und halten diese auf dem neuesten Stand.

Auch wurden angemessene Verfahren umgesetzt, mit denen die Einhaltung gesetzlicher, regulatorischer und vertraglicher Anforderungen mit Bezug auf geistige Eigentumsrechte und der Verwendung von urheberrechtlich geschützten Softwareprodukten sichergestellt ist.

Entsprechend der gesetzlichen, regulatorischen, vertraglichen und geschäftlichen Anforderungen schützen wir Aufzeichnungen und personenbezogene Daten bedarfsgerecht. Jährliche Tätigkeits-berichte des Datenschutzbeauftragten dokumentieren die ergriffenen Maßnahmen.

Wir beachten hierfür die Regelungen Kryptographischer Maßnahmen.
Um den Schutz unserer Informationen und Daten sicher zu stellen, erfolgt regelmäßig eine unabhängige Überprüfung unseres Informationssicherheit- und Datenschutzniveaus, unserer Sicherheits- und Datenschutzrichtlinien, sowie die Einhaltung von technischen Vorgaben.

Anlage 2

Der für den Auftragnehmer bestellte **Datenschutzbeauftragte** ist:

Herr Klaus Foitzick
Vertretung: Herr Michael Plankemann

activeMind AG
Management- und Technologieberatung
Potsdamer Straße 3
D-80802 München

Telefon: +49 (89) 418 56 01-70

E-Mail: datenschutzbeauftragter@wiredminds.de

Verfahrensverzeichnis:
Die ActiveMind AG führt für die wiredminds GmbH ein Verfahrensverzeichnis, dass den gesetzlichen Anforderungen entspricht.

Datengeheimnis:
Alle Mitarbeiter von wiredminds sind über den Arbeitsvertrag an das Datengeheimnis vertraglich gebunden.

Schulung:
Die wiredminds Mitarbeiter werden nachweislich geschult und sind mit den Themen der Datensicherheit und dem Datenschutz vertraut

Anlage 3

Zur **Erteilung von Weisungen** auf Seiten des Auftraggebers sind befugt:

Vorname Nachname

Telefon

E-Mail

Zur **Entgegennahme von Weisungen** auf Seiten des Auftragnehmers sind befugt:

Nicole Widmann
E-Mail: Nicole.Widmann@wiredminds.de
Tel.: 0711 – 585 331 0

Anlage 4

Derzeit werden zur Erbringung des Auftrags folgende Subunternehmer eingesetzt:

Hetzner Online AG
Industriestr. 25

91710 Gunzenhausen
Deutschland

Hinweis:
Technischer Dienstleister; Bezug von Root Servern.
Es besteht KEINE Möglichkeit des Dienstleisters, auf im Auftrag verarbeitete Daten zuzugreifen.