

Vertrag über die Auftragsverarbeitung personenbezogener Daten in WiredMinds LeadLab nach DSGVO

**Bitte senden Sie den unterzeichneten Vertrag an
datenschutz@wiredminds.de**

Ihr Team der WiredMinds GmbH

Telefon: 0049 711 585 331 0

E-Mail: datenschutz@wiredminds.de

Web: www.wiredminds.de

Einleitung

Unsere Software LeadLab erfüllt alle Vorgaben der DSGVO. WiredMinds und seine Lösungen halten alle Vorschriften und Regelungen des Datenschutzes ein. Das gewährleisten wir - schon immer und besonders heute.

Die Reichweitenmessung Ihrer Webseite durch den Einsatz von WiredMinds LeadLab bedarf keiner Zustimmung Ihrer Webseitenbesucher. Das sagen nicht nur wir, sondern auch das für uns zuständige Landesamt für Datenschutz und Informationssicherheit.

<https://www.baden-wuerttemberg.datenschutz.de/faq-zu-cookies-und-tracking-2/>

Begründung

- Wir erheben und Speichern keine Daten auf der Endeinrichtung des Endnutzers (§ 25 TTDSG)
- Wir erheben die IP-Adresse des Webseitenbesuchers aus dem TCP/IP-Protokoll
- Die IP-Adresse dient dem einmaligen, temporären Abgleich gegen unsere Firmendatenbank
- Diesen Prozess stützen wir auf Art. 6 Abs. 1 (f) DSGVO
- Erst nach erfolgreichem Abgleich gegen unsere Firmendatenbank erheben wir Besucherdaten.
- User Fokus liegt auf der Ermittlung der B2B-relevante Webseitenbesucher.
- Wir behalten Ihre Daten in Deutschland
- Wir halten uns an alle Gesetze und Vorgaben der DSGVO

Für die Reichweitenmessung in Ihrem Auftrag benötigen wir diesen AVV, weil

- wir in Ihrem Auftrag handeln und für Ihre Webseite eine Reichweitenmessung durchführen
- wir für Sie LeadLab-Zugangsdaten einrichten und dabei die personenbezogenen Daten Ihrer Mitarbeiter verarbeiten
- wir Ihnen die Möglichkeit geben, in LeadLab Reports einzurichten, die Sie an eine E-Mail-Adresse (personenbezogener Wert) Ihrer Vertriebsmitarbeiter senden können

Mehr Informationen und Dokumente finden Sie auf:

wiredminds.de/datenschutz oder schreiben Sie direkt an datenschutz@wiredminds.de

"Mit WiredMinds gehen Sie kein Risiko ein. Ihre Daten sind nur Ihre Daten und deren Verarbeitung ist bei uns sicher und dokumentiert. Das war schon immer so und gilt auch im Rahmen der DSGVO".

Albert Denz, Geschäftsführer
WiredMinds GmbH

Vertragspartner

Auftragnehmer

Auftraggeber (bitte Daten eintragen)

WiredMinds GmbH

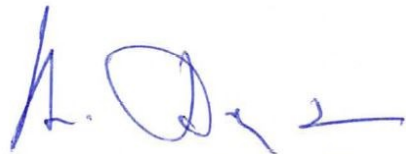
Lindenspürstr. 32

70176 Stuttgart

Vertreten durch:

Vertreten durch: (Bitte Daten eintragen)

Ort, Datum



Albert Denz
Geschäftsführer

1 Gegenstand und Dauer der Verarbeitung

1.1. Gegenstand

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

Bezeichnung des Vertrages:
Bitte übernehmen Sie in das Feld den entsprechenden
Produktnamen „Testaccount“ „LeadLab Lite“ „LeadLab“

Datum des Vertragsabschlusses:

1.2. Dauer

Die Verarbeitung beginnt am

Bitte tragen Sie den gewünschte Vertragsbeginn bzw. den
Beginn der Testphase in das Feld ein:

und erfolgt auf unbestimmte Zeit bis zur Beendigung (Punkt 10) dieses Vertrags oder des Hauptvertrags durch eine Partei.

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

2.1. Art und Zweck der Verwendung

Die Verarbeitung ist folgender Art:

Einsatz einer Zählpixeltechnologie der WiredMinds GmbH auf der Webseite des Auftraggebers zur Erfassung der IP-Adresse aller Webseitenbesucher und einem einmaligen temporärer Abgleich der IP-Adresse gegen die Firmendatenbank der WiredMinds GmbH. Ordnen und sortieren der Besuche nach B2B-relevanten Besuchen und herausfiltern aller Besuche von natürlichen Personen. Eine Speicherung, Anpassung oder Veränderung der IP-Adresse findet nicht statt. Das Besuchsverhalten der B2B-relevanten Unternehmen wird aufgezeichnet, dem Auftraggeber in LeadLab bereitgestellt und kann zur Reichweitenmessung durch den Auftraggeber verwendet werden.

Die Verarbeitung dient folgendem Zweck:

- Erkennung und Filterung möglicherweise identifizierbarer Webseitenbesucher.
- Wartung der bereitgestellten Lösung inkl. Verwaltung der Benutzer beim Kunden

2.2. 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

2.3. Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

- Mitarbeiter des Auftraggebers (Benutzer von LeadLab)
- Webseitenbesucher

3 Pflichten des Auftragnehmers

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vereinbart oder angewiesen, es sei denn, es besteht eine gesetzliche Verpflichtung zur Verarbeitung.
- (2) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren und eingesetzte Mitarbeiter entsprechend zu verpflichten.
- (3) Der Auftragnehmer wird den Auftraggeber bei der Erfüllung von datenschutzrechtlichen Pflichten oder im Rahmen von Kontrollen, etwa durch Aufsichtsbehörden, soweit erforderlich unterstützen.
- (4) Auskünfte darf der Auftragnehmer nur nach Zustimmung durch den Auftraggeber erteilen. An ihn gerichtete Anfragen wird er an den Auftraggeber weiterleiten.
- (5) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz.
- (6) Die Auftragsverarbeitung erfolgt ausschließlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen erfolgen.

4 Technische und organisatorische Maßnahmen

- (1) Die vom Auftragnehmer umgesetzten Datensicherheitsmaßnahmen sind in Anhang 1 beschrieben.
- (2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird.
- (3) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen.
- (4) Die Verarbeitung von Daten im HomeOffice ist zulässig. Vom Auftragnehmer ist sicherzustellen, dass dabei die Datensicherheit nicht beeinträchtigt wird und die Kontrollrechte des Auftraggebers uneingeschränkt ausgeübt werden können.
- (5) Der Auftragnehmer führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten.

5 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.

6 Unterauftragsverhältnisse

- (1) Der Auftraggeber stimmt 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. 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.

7 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 erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

8 Mitteilungspflichten

- (1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit.
- (2) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

9 Weisungen

- (1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.
- (2) 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.

10 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.
- (2) 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.

11 Haftung

- (1) 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.
- (2) Nummer (1) gilt nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

12 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.

Anlagen

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 sichergestellt. 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-Sicherheitsaufgaben 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 Wechselträgern, 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 berechnigte 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 von Benutzern, der die Zuordnung von Zugangsrechten 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 Anwendungsschutzmaßnahmen 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 bei unserem Hosting-Partner sichergestellt
- 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 über einen automatischen Screensaver und eine automatische Verschlüsselung der Festplatte geschützt
- Richtlinien für Clean Desk und Bildschirm Sperren 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
- Anzahl der RDP-Sessions der einzelnen Terminal-Server
- Durchsatz und Auslastung der Firewall
- Prüfung der Erreichbarkeit aller Server ist über Monitoring möglich
- 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 (z. B. CRM Anbieter).

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 (Schutzklasse 1_E2) 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 und 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, selbstaufgelegten 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 Tätigkeitsberichte 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 Informationssicherheits- und Datenschutzniveaus, unserer Sicherheits- und Datenschutzrichtlinien, sowie die Einhaltung von technischen Vorgaben.

Anlage 2

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

Datenschutzbeauftragter der WiredMinds GmbH
c/o activeMind
Potsdamer Str. 3
80802 München
Tel. 089-418560170

Telefon: +49 (0)89 91 92 94 - 900
www.activemind.de

E-Mail: datenschutzbeauftragter@wiredminds.de

Allgemein:

Die Activemind AG führt für die WiredMinds GmbH ein Verzeichnisse, das den gesetzlichen Anforderungen entspricht. Alle Mitarbeiter von WiredMinds sind über den Arbeitsvertrag an das Datengeheimnis vertraglich gebunden. Die WiredMinds Mitarbeiter werden nachweislich geschult und sind mit den Themen der Datensicherheit und dem Datenschutz vertraut

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

1. Datenschutzbeauftragter

Vorname Nachname oder Funktionsbezeichnung

Telefon

E-Mail

Anlage 3

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

1. Weisungsbefugter

Vorname Nachname oder Funktionsbezeichnung

Telefon

E-Mail

2. Weisungsbefugter (optional)

Vorname Nachname oder Funktionsbezeichnung

Telefon

E-Mail

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

Nicole Widmann

E-Mail: nicole.widmann@wiredminds.de

Tel.: 0711 – 585 331 310

Datenschutzkoordinator

E-Mail: datenschutz@wiredminds.de

Tel.: 0711 – 585 331 375

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.