Auftragsverarbeitungsvertrag nach Art. 28 III DS-GVO

Dieser Auftragsverarbeitungsvertrag (AVV) regelt die Rechte und Pflichten der Vertragsparteien im Rahmen der Verarbeitung personenbezogener Daten durch den Auftragnehmer (Auftragsverarbeiter) im Auftrag des Auftraggebers (Verantwortlicher). Die Vertragsparteien verpflichten sich, die Regelungen der Datenschutz-Grundverordnung (DSGVO), insbesondere die Anforderungen aus Artikel 28 DSGVO, einzuhalten.

Der Auftragnehmer verpflichtet sich, personenbezogene Daten ausschließlich auf Grundlage dokumentierter Weisungen des Auftraggebers und im Rahmen der vertraglich vereinbarten Leistungen zu verarbeiten. Darüber hinaus stellt der Auftragnehmer sicher, dass er geeignete technische und organisatorische Maßnahmen getroffen hat, um die Sicherheit der Daten zu gewährleisten und die Rechte der betroffenen Personen zu wahren.

Die Vertragsparteien

- im Folgenden: Auftraggeber -

_____

_____

_____

_____

- im Folgenden: Auftragnehmer -

SoftTec GmbH
Hindelanger Straße 35
87527 Sonthofen
Deutschland

schließen folgenden Vertrag:

§1 Gegenstand

1.1 Der Auftragnehmer verarbeitet personenbezogene Daten (Art. 4 Nr. 2 DSGVO) im Auftrag des Auftraggebers nach Art. 28 DSGVO. Der Inhalt des Auftrags, die Kategorien betroffener Personen und Datenarten sowie der Zweck der Verarbeitung sind in Anlage 1 des Vertrages geregelt.

1.2 Die Verarbeitung der Daten durch den Auftragnehmer findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, einem Mitgliedsstaat der EU oder einem Vertragsstaat des EWR-Abkommens statt. Die Verarbeitung außerhalb der genannten Staaten erfolgt nur unter den Voraussetzungen von Art. 44 ff. DSGVO mit vorheriger Zustimmung des Auftraggebers.

1.3 Die Vergütung wird im jeweiligen Projekt festgelegt.

§2 Vertragslaufzeit und Kündigung

Dieser Auftragsverarbeitungsvertrag wird auf unbestimmte Zeit geschlossen und bleibt so lange in Kraft, bis er von einer der Vertragsparteien gemäß den in den Allgemeinen Geschäftsbedingungen (AGB) der SoftTec GmbH festgelegten Kündigungsbedingungen gekündigt wird. Diese können unter https://www.softtec.de/agbs eingesehen werden.

§3 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

3.1 Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er ist für die Beurteilung der Rechtmäßigkeit von Datenverarbeitungsvorgängen nach Art. 6 I DSGVO und die Wahrung der Betroffenenrechte nach Art. 12 bis 22 DSGVO mit Unterstützung des Auftragnehmers zuständig. Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Betroffenenanfragen nachzukommen, insbesondere die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Der Auftragnehmer ist verpflichtet, alle Anfragen zeitnah an den Auftraggeber weiterzuleiten.

3.2 Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf die Datenverarbeitung, insbesondere Art und Umfang gegenüber dem Auftragnehmer zu. Er kann insbesondere die unverzügliche Löschung, Berichtigung, Sperrung oder Herausgabe der vertragsgegenständlichen Daten verlangen. Der Auftragnehmer ist verpflichtet, den Weisungen des Auftraggebers Folge zu leisten, sofern er nicht aufgrund zwingender europäischer oder mitgliedsstaatlicher Rechtsvorschriften zur Verarbeitung der personenbezogenen Daten verpflichtet ist. Der Auftraggeber benennt eine oder mehrere weisungsberechtigten Personen; Änderungen sind unverzüglich mitzuteilen.

3.3 Verfahrensänderungen, die die technische Durchführung oder die Organisation der Datenverarbeitung betreffen, sind zwischen dem Auftraggeber und dem Auftragnehmer abzustimmen. Über den Verarbeitungsgegenstand, also die Art und den Umfang der verarbeiteten personenbezogenen Daten, entscheidet allein der Auftraggeber.

3.4 Der Auftragnehmer macht den Auftraggeber unverzüglich darauf aufmerksam, wenn eine erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften

verstößt (Art. 28 III 3 DSVGO). Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragnehmer substantiiert anzweifelt, ist der Auftragsnehmer berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert.

3.5 Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format zu erteilen. Mündliche Weisungen sind auf Verlangen des Auftragnehmers schriftlich oder in einem elektronischen Format durch den Auftraggeber zu bestätigen. Der Auftragnehmer hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren.

3.6 Der Auftragnehmer ist nicht berechtigt, die personenbezogenen Daten für eigene Zwecke zu nutzen.

§4 Kontrollbefugnisse des Auftraggebers

4.1 Der Auftraggeber bleibt im Rahmen der Datenverarbeitung für die Einhaltung der geltenden Datenschutzgesetze, insbesondere der Anforderungen aus Art. 28 DSGVO, verantwortlich. Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig und in angemessenem Umfang zu überprüfen oder durch einen beauftragten Dritten prüfen zu lassen. Der Auftragnehmer verpflichtet sich, diese Überprüfungen zu dulden und in zumutbarem Umfang zu unterstützen. Der Auftragnehmer hat alle notwendigen Auskünfte zu erteilen und dem Auftraggeber die Einsichtnahme in die relevanten Daten, Datenverarbeitungsprogramme und -systeme zu gewähren. Er ist weiterhin verpflichtet, Vor-Ort-Kontrollen nach vorheriger Ankündigung durch den Auftraggeber zu ermöglichen, sofern dies zur Erfüllung der Pflichten aus Art. 28 DSGVO erforderlich ist.

4.2 Der Auftraggeber sorgt dafür, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragnehmers nicht weiter als unbedingt erforderlich beeinträchtigen. Insbesondere sollten Vorortkontrollen grundsätzlich zu den üblichen Geschäftszeiten und nach Terminvereinbarung mit angemessener Fristsetzung erfolgen, sofern der Kontrollzweck keiner vorherigen Ankündigung entgegensteht.

4.3 Das Ergebnis der Kontrolle ist von beiden Vertragsparteien zu protokollieren.

4.4 Die entstehenden Kosten sowohl auf Seiten des Auftraggebers als auch auf Seiten des Auftragnehmers für die Vorbereitung und Durchführung einer Überprüfung durch oder im Auftrag des Auftraggebers trägt der Auftraggeber.

§5 Pflichten des Auftragnehmers

5.1 Der Auftragsnehmer hält bei der Auftragsverarbeitung sämtliche gesetzliche Vorschriften ein, er hat insbesondere die notwendigen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO zu ergreifen und das erforderliche Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 II DSGVO zu führen.

5.2 Die Verarbeitung der Daten durch den Auftragsnehmer erfolgt nur auf Grundlage der vertraglichen Vereinbarung und den erteilten Weisungen des Auftraggebers. Eine abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedsstaatlicher Rechtsvorschriften zulässig. Ist eine Verarbeitung wegen zwingenden Rechts erforderlich, teilt der Auftragnehmer dies dem Auftraggeber vor der Verarbeitung schriftlich mit, sofern das betreffende Recht einer solchen Mitteilung nicht entgegensteht.

5.3 Ist der Auftragnehmer zur Benennung eines Datenschutzbeauftragten verpflichtet, bestätigt er, dass er einen solchen ausgewählt hat und sichert zu, diesen unter Angabe der Kontaktdaten zu benennen. Sofern der Auftragnehmer nicht zur Benennung eines Datenschutzbeauftragten verpflichtet ist, hat einen Ansprechpartner in Sachen Datenschutz zu benennen. Änderungen sind unverzüglich mitzuteilen.

5.4 Nach Vertragsende sind alle personenbezogenen Daten nach Wahl des Auftraggebers entweder zu löschen oder herauszugeben, und die vorhandenen Kopien sind zu löschen, sofern nicht nach europäischen oder mitgliedsstaatlichen Rechtsvorschriften eine Verpflichtung zur Speicherung der Daten besteht. Die Kosten, die nach Vertragsbeendigung durch die Herausgabe oder Löschung von Daten entstehen, trägt der Auftraggeber.

§6 Technische und organisatorische Maßnahmen

6.1 Der Auftragnehmer gewährleistet ein angemessenes Schutzniveau für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen, durch geeignete technische und organisatorische Maßnahmen im Sinne des Art. 32 DSGVO. Diese Maßnahmen wurden unter Berücksichtigung des Standes der Technik sowie der Risiken der Verarbeitung ausgewählt und mit dem Auftraggeber abgestimmt. Die aktuell gültigen Maßnahmen sind in Anlage 2 festgehalten, welche regelmäßig aktualisiert und dem Auftraggeber zur Verfügung gestellt wird.

6.2 Der Auftragnehmer überprüft und bewertet die technischen und organisatorischen Maßnahmen, mindestens jedoch einmal jährlich, und passt diese bei Bedarf an, um den anerkannten Stand der Technik und das vereinbarte Schutzniveau zu wahren. Alle Änderungen werden dokumentiert und dem Auftraggeber auf Anfrage zur Verfügung gestellt. Wesentliche Änderungen, die eine Anpassung der Maßnahmen erfordern, werden mit dem Auftraggeber abgestimmt.

§7 Einsatz von Unterauftragsverarbeitern (Subunternehmern)

7.1 Der Auftragnehmer ist nur mit Zustimmung des Auftragsgebers zum Einsatz von Subunternehmern berechtigt, Art. 28 II DSGVO. Die Subunternehmer müssen ausdrücklich benannt werden. Die bereits bestehenden Subunternehmerverhältnisse, welche in Anlage 3 des Vertrages beigefügt sind, gelten als bestätigt mit Unterzeichnung dieses Vertrages. Beabsichtigt der Auftragnehmer den Einsatz weiterer Subunternehmer, wird er dies dem Auftraggeber in schriftlicher Form mitteilen, damit dieser deren Einsatz prüfen kann. Erfolgt keine Zustimmung durch den Auftraggeber, dürfen die betroffenen Subunternehmer nicht eingesetzt werden. Die Zustimmung kann nur unter Angabe gewichtiger Gründe, die Anhaltspunkte für ein Unterschreiten des von der DSGVO vorgegeben Datenschutzniveaus enthalten, verweigert werden. Im Falle einer solchen Verweigerung bemühen sich die Vertragspartner um die Herbeiführung

einer interessengerechten Einigung. Im Rahmen dessen kann auch ein Unterauftragnehmer als Alternative vorgeschlagen werden, dessen Dienstleistung im Vergleich zum abgelehnten Unterauftragnehmer gleichwertig ist und der insbesondere die an ihn adressierten Vorgaben aus Art. 28 DSGVO erfüllt.

7.2 Die Auswahl eines Subunternehmers erfolgt durch den Auftragsnehmer unter Beachtung der gesetzlichen und vertraglichen Vorgaben. Nebenleistungen, die der Auftragnehmer zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt, stellen keine Unterauftragsverhältnisse dar. Der Auftragnehmer wird jedoch auch bei diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards gewährleisten.

7.3 Die vertraglichen Vereinbarungen mit Subunternehmern haben den Anforderungen zu Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrags und der gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten zu entsprechen. Dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO. Dem Auftraggeber sind Kontroll- und Überprüfungsrechte nach Art. 28 III lit.h DSGVO einzuräumen.

7.4 Die Weiterleitung von Daten an einen Subunternehmer ist nur zulässig, wenn der Subunternehmer hinreichende Garantien dafür bietet, dass er geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO ergriffen hat und seine Beschäftigten auf die Vertraulichkeit verpflichtet wurden. Der Auftragnehmer stellt sicher, dass diese Anforderungen durch vertragliche Vereinbarungen mit dem Subunternehmer eingehalten werden.

§8 Geheimhaltungspflicht

Der Auftragnehmer verpflichtet sich, alle im Rahmen dieses Vertrages erlangten Geschäftsgeheimnisse sowie die personenbezogenen Daten des Auftraggebers streng vertraulich zu behandeln und nur im Rahmen der vertraglich vereinbarten Leistungen zu verwenden. Diese Verpflichtung bleibt auch nach Beendigung des Vertragsverhältnisses bestehen. Der Auftragnehmer stellt sicher, dass sämtliche Personen, die Zugang zu diesen Daten haben, entsprechend zur Vertraulichkeit verpflichtet sind. Die zur Verarbeitung der Daten befugten Personen dürfen erst nach Unterwerfung unter die Vertraulichkeitspflicht Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

§9 Schlussbestimmungen

9.1 Änderungen und Ergänzungen sowie Nebenabreden dieser Vereinbarung und aller ihrer Bestandteile bedürfen zu ihrer Wirksamkeit einer schriftlichen Vereinbarung.

9.2 Verstöße gegen diesen Vertrag, gegen Weisungen oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen. Das Gleiche gilt bei Vorliegen eines Verdachts auf einen Verstoß.

9.3 Bei Änderungen der Datenschutz-Grundverordnung (DSGVO) während der Vertragslaufzeit gelten die Verweise in diesem Vertrag automatisch auch für die entsprechenden Bestimmungen der jeweils gültigen Nachfolgeregelungen.

9.4 Bei Unwirksamkeit einzelner Teile dieser Vereinbarung, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

9.5 Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

Für den Auftraggeber	**Für den Auftragnehmer**
	Sonthofen, den 01.12.2024
_____	
Ort, Datum	Unterschrift
_____	
Unterschrift	

Anlage 1
Auftragsdetails

Dieser Vertrag umfasst die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers im Rahmen der vertraglich vereinbarten Leistungen aus dem Hauptvertrag. Insbesondere betrifft dies folgende Leistungen:

- Durchführung von Wartungsarbeiten, die zur Sicherstellung der Funktionsfähigkeit und zur Anpassung der vom Auftragnehmer gelieferten Software erforderlich sind,
- Bereitstellung von Unterstützung und Korrekturmaßnahmen im Zusammenhang mit der vom Auftragnehmer gelieferten Software.

Im Rahmen der vertraglichen Leistungserbringung werden regelmäßig folgende Datenarten verarbeitet:

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- Daten, die in der Software des Auftragsgebers vom Auftraggeber erfasst wurden

Bei dem Kreis der von der Datenverarbeitung betroffenen Personen handelt es sich um:

- Kunden: Personen oder Unternehmen, die Leistungen oder Produkte des Auftraggebers in Anspruch nehmen.
- Mitarbeiter des Kunden: Beschäftigte der Kundenunternehmen, die im Rahmen der vertraglichen Leistungen in Kontakt mit dem Auftragnehmer stehen oder dessen Software nutzen.
- Gäste: Personen, die ohne bestehende vertragliche Beziehung zu den Kunden oder zum Auftraggeber temporär Kontakt zu den Systemen oder Räumlichkeiten des Auftraggebers haben (z. B. zum Beispiel beim Einchecken über den Checkin-Kiosk oder der Benutzung der Gäste-App/des Digitalen Meldescheins um die Meldedaten zu hinterlegen).

Der Zugriff auf die betroffenen Daten geschieht in folgender Weise:
Im Rahmen der Wartung wird definiert, welche Systeme und Anwendungen durch den Auftragnehmer installiert und betreut werden. Sofern der Auftragnehmer die Wartung und/oder Pflege der IT-Systeme auch im Wege der Fernwartung durchführt, ist der Auftragnehmer verpflichtet, dem Auftraggeber eine wirksame Kontrolle der Fernwartungsarbeiten zu ermöglichen. Dies erfolgt durch den Einsatz der Fernwartungssoftware TeamViewer. Wenn der Auftraggeber bei Fernwartungsarbeiten nicht wünscht, die Tätigkeiten an einem Monitor o.ä. Gerät zu beobachten, wird der Auftragnehmer die von ihm durchgeführten Arbeiten in geeigneter Weise dokumentieren. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

Anlage 2
Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO

Grundsätzliche Maßnahmen

- Grundsätze des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)

  Bei der SoftTec GmbH wird der Schutz personenbezogener Daten im Rahmen des Möglichen und unter Berücksichtigung des Stands der Technik sowie der verfügbaren Ressourcen umgesetzt. Von Beginn an legen wir Wert darauf, Datenschutz und Sicherheit in die Gestaltung und Auswahl von Hardware, Software und Verfahren einzubinden (Privacy by Design und Privacy by Default). Dabei streben wir an, potenzielle Risiken für die Rechte und Freiheiten von Personen, soweit vorhersehbar, angemessen zu reduzieren.

- Verpflichtung zur Vertraulichkeit und Sensibilisierung der Mitarbeiter

  Mitarbeiter der SoftTec GmbH sind hinsichtlich des Datenschutzes auf Verschwiegenheit verpflichtet, werden regelmäßig belehrt und über mögliche Haftungsfolgen instruiert. Spezielle Regelungen existieren für Mitarbeiter, die außerhalb betriebsinterner Räumlichkeiten tätig sind oder Privatgeräte für betriebliche Zwecke verwenden, um den Schutz der Daten und die Sicherung der Rechte von Auftraggebern in Auftragsverarbeitungen zu gewährleisten.

- Verwaltung und Entzug von Zugangs- und Berechtigungsrechten

  Die an Mitarbeiter ausgegebenen Schlüssel, Zugangskarten oder Codes sowie die Berechtigungen zur Verarbeitung personenbezogener Daten werden bei ihrem Ausscheiden aus dem Unternehmen oder bei einem Wechsel der Zuständigkeiten überprüft und angepasst bzw. entzogen. Dadurch wird sichergestellt, dass nur autorisierte Personen Zugang zu sensiblen Bereichen und Daten haben.

Zutrittskontrolle

- Sicherheitsmaßnahmen zum Schutz physischer und elektronischer Daten

  Die Verarbeitung personenbezogener Daten bei der SoftTec GmbH erfolgt überwiegend elektronisch. Für den Fall, dass personenbezogene Daten in physischer Form vorliegen und eines speziellen Zutrittsschutzes bedürfen, wird dieser durch geeignete Maßnahmen wie den Verschluss in sicheren Schränken oder die Verwahrung in abschließbaren Räumen sichergestellt. Zusätzlich wird gewährleistet, dass Unbefugte keinen Zutritt zu den Datenverarbeitungsanlagen erhalten, indem diese durch ein Chipkarten- und Transponder-Schließsystem geschützt sind. Diese Maßnahmen gewährleisten, dass nur befugte Personen

- Zugang haben und minimieren das Risiko eines unberechtigten Zugriffs.

  Regelungen zum Zugang betriebsfremder Personen und externer Dienstleister Betriebsfremde Personen dürfen die Räumlichkeiten der SoftTec GmbH grundsätzlich nur in Begleitung eines autorisierten internen Mitarbeiters betreten. Ausnahmen bestehen für externe Dienstleister, wie zum Beispiel

Reinigungspersonal, die sorgfältig ausgewählt, speziell eingewiesen und kontrolliert werden, um den Schutz sensibler Informationen sicherzustellen.

- Chipkarten-/Transponder-Schließsystem

  Bei SoftTec GmbH wird ein Chipkarten- bzw. Transponder-Schließsystem eingesetzt, das sicherstellt, dass nur autorisierte Mitarbeiter Zugang zu den Räumlichkeiten und sensiblen Bereichen erhalten. Jeder Mitarbeiter erhält eine personalisierte Chipkarte oder einen Transponder, der den Zutritt zu den entsprechenden Zonen ermöglicht. Unbefugten Personen ist der Zugang ohne entsprechende Berechtigung verwehrt, wodurch der Schutz sensibler Daten gewährleistet wird.

Zugangskontrolle / Zugriffskontrolle

- Verwendung personenbezogener Benutzeraccounts zur Zugriffsnachverfolgbarkeit

  Bei der SoftTec GmbH werden ausschließlich personenbezogene Benutzeraccounts verwendet. Jeder Mitarbeiter erhält einen individuellen Zugang, der nur von dieser Person genutzt werden darf. Dadurch wird sichergestellt, dass jeder Zugriff auf die IT-Systeme eindeutig einer Person zugeordnet werden kann, was eine effektive Überwachung und Nachverfolgbarkeit aller Aktivitäten ermöglicht. Unbefugte Nutzung oder Missbrauch von Accounts wird somit verhindert.

- VPN-Einsatz zur Absicherung externer Zugriffe auf interne Systeme

  Bei der SoftTec GmbH wird VPN-Technologie (Virtual Private Network) eingesetzt, um den sicheren Zugriff auf interne Systeme und personenbezogene Daten von außerhalb des Unternehmensnetzwerks zu gewährleisten. Mitarbeiter, die remote arbeiten oder auf sensible Daten zugreifen müssen, nutzen das VPN, um eine verschlüsselte Verbindung herzustellen und den Datentransfer vor unbefugtem Zugriff oder Manipulation zu schützen. Zusätzlich wird die Sicherheit durch Bildschirmsperren nach einer definierten Inaktivitätszeit gewährleistet, um unbefugten Zugriff zu verhindern. Es gibt jedoch Ausnahmen, wenn Vertriebsmitarbeiter direkt mit Personen in Kontakt sind und durch ihre Präsenz und Aufmerksamkeit die Sicherheit gewährleisten können. Datenträger und Unterlagen mit sensiblen Informationen werden stets sicher aufbewahrt, um einen umfassenden Schutz zu gewährleisten.

- Erhöhte Zugangssicherheit durch Zwei-Faktor-Authentifizierung (2FA)

  Bei der SoftTec GmbH erfolgt die Authentifizierung standardmäßig durch eine Zwei-Faktor Authentifizierung (2FA) für erhöhten Schutz. Die Kombination von Benutzername und Passwort wird nur verwendet, wenn das jeweilige System oder Produkt eine 2FA nicht unterstützt. Wo möglich, wird neben dem Passwort ein weiterer Authentifizierungsfaktor, wie ein Code aus einer Authentifizierungs-App oder ein Hardware-Token, eingesetzt. Damit stellen wir sicher, dass der Zugriff auf sensible Bereiche und Systeme bestmöglich vor unbefugten Zugriffen geschützt ist.

- Berechtigungskonzept nach dem Prinzip der minimalen Rechte (Least Privilege Principle)

  Bei der SoftTec GmbH werden Berechtigungs- und Authentifizierungskonzepte nach dem Prinzip der minimalen Rechte (Least Privilege Principle) umgesetzt, um

sicherzustellen, dass Mitarbeiter nur auf die Daten und Systeme zugreifen können, die für ihre Aufgaben erforderlich sind. Dies minimiert das Risiko von Datenmissbrauch und unbefugtem Zugriff.

- Passwortsicherheitsrichtlinien gemäß branchenüblichen Standards

  Die SoftTec GmbH setzt strenge Mindestanforderungen an die Passwortsicherheit um, die sich an den branchenüblichen Standards orientieren und den Schutz von personenbezogenen Daten sowie sensiblen Systemen sicherstellen.

Weitergabekontrolle

- Prüfung der Pseudonymisierung zur sicheren Datenverarbeitung

  Die SoftTec GmbH prüft die Möglichkeit der Pseudonymisierung von personenbezogenen Daten, um, sofern technisch und organisatorisch machbar, das Risiko für betroffene Personen zu minimieren. Dabei wird der Einsatz von Pseudonymen erwogen, um direkte Identifikationsmerkmale zu reduzieren und gleichzeitig eine sichere Datenverarbeitung zu gewährleisten.

Verfügbarkeitskontrolle / Integrität

- Betrieb und Sicherheitsstandards europäischer Rechenzentren

  Die SoftTec GmbH betreibt alle ihre Server in Rechenzentren innerhalb Europas, die nach DIN/ISO 27001 zertifiziert sind. Dies garantiert höchste Sicherheitsstandards in Bezug auf Datenverfügbarkeit, Vertraulichkeit und Integrität sowie die Einhaltung der geltenden Datenschutzbestimmungen.

- Kontrolliertes Backup- und Recoverykonzept zur Sicherstellung der Geschäftskontinuität

  Die SoftTec GmbH verfügt über ein ständig kontrolliertes Backup- und Recoverykonzept, das sicherstellt, dass alle wichtigen Daten regelmäßig gesichert und im Falle eines Systemausfalls oder Datenverlusts schnell und vollständig wiederhergestellt werden können. Dieses Konzept schützt vor Datenverlust und gewährleistet die Geschäftskontinuität.

Gewährleistung des Zweckbindungs-/Trennungsgebotes

- Trennung von Produktiv- und Testsystemen zum Schutz sensibler Daten

  Die SoftTec GmbH stellt die Einhaltung des Zweckbindungs- und Trennungsgebotes durch eine klare Trennung von Produktiv- und Testsystemen in ihren Softwarelösungen, einschließlich des CRM-Systems, sicher. Die Mandantentrennung wird durch den Einsatz physisch getrennter Softwareprojekte gewährleistet. In den Testumgebungen kommen ausschließlich fiktive Daten zum Einsatz, um sicherzustellen, dass keine sensiblen Informationen unbeabsichtigt verarbeitet werden.

Anlage 3
Liste der bestehenden Subunternehmer

1. Ruthardt Systemhaus GmbH
   Friedrich-List-Straße 34
   70771 Leinfelden-Echterdingen
   +49 (0) 711 / 2526910
   info@ruthardt-system.de
   https://www.ruthardt-system.de
   Zweck: Externe IT Dienstleistung

2. STRATO AG
   Otto-Ostrowski-Straße 7
   10249 Berlin
   +49 (0) 30 / 3001460
   impressum@strato.de
   https://www.strato.de
   Zweck: Hosting

3. IONOS SE
   Elgendorfer Str. 57
   56410 Montabaur
   +49 (0) 721 / 1705522
   info@ionos.de
   https://www.ionos.de
   Zweck: Hosting

4. efsta IT Services GmbH
   Pachergasse 17 / Top 11
   4400 Steyr
   +43 (0) 7252 / 930780
   office@efsta.eu
   https://www.efsta.eu
   Zweck: Rechtskonforme Fiskalisierung

5. CHT GmbH & Co. KG
   Werner-von-Siemens-Str. 6
   86159 Augsburg
   +49 (0) 821 / 4504140
   post@cht.de
   https://www.cht.de
   Zweck: Externe Datensicherung

6. TERRA CLOUD GmbH
   Hankamp 2
   32609 Hüllhorst
   +49 (0) 5744 / 9440
   support@terracloud.de
   https://terracloud.de
   Zweck: Hosting und Externe Datensicherung

7. WORTMANN AG
   Bredenhop 20
   32609 Hüllhorst

+49 (0) 5744 / 9440
info@wortmann.de
https://www.wortmann.de
Zweck: Hosting und Externe Datensicherung

8. Microsoft Ireland Operations, Ltd.
One Microsoft Place
South County Business Park
Leopardstown
Dublin 18, D18 P521, Ireland
01806 / 672255
kunden@microsoft.com
https://www.microsoft.com
Zweck: Hosting und Externe Datensicherung