

End User Licence Agreement (EULA) Can Do (Can Do Software) Service

<p>Diese Bedingungen (nachstehend „EULA“) sind die Grundlage für die Nutzung, der von der Can Do GmbH, Implerstr. 26, 81371 München angebotenen Online-Services (nachstehend „Can Do“ oder “Can Do Software“) durch den Vertragspartner (nachstehend „Kunde“).</p>	<p>These conditions (hereinafter "EULA") form the basis for the use of the online services (hereinafter "Can Do" or Can Do Software) offered by Can Do GmbH, Implerstr. 26, 81371 Munich by the contractual partner (hereinafter "Customer").</p>
<p>Diese EULA gelten ausschließlich; entgegenstehende oder von diesen Geschäftsbedingungen abweichende Bedingungen des Kunden werden nicht anerkannt, es sei denn, die Can Do GmbH stimmt ausdrücklich schriftlich ihrer Geltung zu.</p>	<p>These EULA shall apply exclusively; any terms and conditions of the customer which conflict with or deviate from our terms and conditions set forth herein shall not be recognised unless Can Do GmbH expressly agrees to their validity in writing.</p>
<p>Diese EULA regeln die Bereitstellung der Can Do Software durch die Can Do GmbH an den Kunden. Mit der Can Do Software stellt die Can Do GmbH dem Kunden die technische Möglichkeit und Berechtigung, auf die Can Do Software, welche auf einem Server im Namen der Can Do GmbH betrieben wird, über das Internet direkt über Webbrowser zuzugreifen und die Funktionalitäten der Can Do Software im Rahmen dieser Vereinbarungen zu nutzen.</p>	<p>These EULAs govern the provision of the Can Do Software by Can Do GmbH to customer. With the Can Do Software, Can Do GmbH provides the customer with the technical possibility and authorization to access the Can Do Software, which is operated on a server operated in the Name of Can Do GmbH, via the Internet directly via web browser and to use the functionalities of the Can Do Software within the framework of this agreement.</p>
<p>Art und Umfang der Funktionen der Can Do Software sind unter https://www.can-do.de abschließend beschrieben. Die vertraglichen Leistungen ergeben sich aus der jeweiligen (elektronischen) Bestellung des Kunden.</p>	<p>The nature and extent of the Can Do Software functions are described in detail under https://www.can-do.de/en The contractual services are agreed in the respective (electronic) order of the customer.</p>
<p>Die durchschnittliche Verfügbarkeit während der Betriebszeiten beträgt im Verantwortungsbereich der Can Do GmbH 99 % im Monatsmittel. Nicht in die Berechnung der Verfügbarkeit fallen die regulären Wartungsfenster des Systems. Während dieser Zeiten kann die Anwendung dennoch, ggf. mit Unterbrechungen und Einschränkungen verfügbar sein; es besteht jedoch kein Anspruch auf Nutzung. Falls in den Betriebszeiten Wartungsarbeiten erforderlich werden und die Anwendung deshalb nicht zur Verfügung steht, wird die Can Do GmbH den Kunden hierüber nach Möglichkeit rechtzeitig informieren.</p>	<p>The average availability during the operating hours in the area of responsibility of Can Do GmbH shall be 99 % as a monthly average. Scheduled maintenance times of the system, are not included in the calculation of availability. During these times, the application may still be available, with interruptions and restrictions where applicable; however, there is no entitlement to use. If maintenance work becomes necessary during operating hours and the application is therefore not available, Can Do GmbH will inform the customer of this in good time if possible.</p>
<p>Der Kunde wird Fehler der vertragsgegenständlichen Leistungen der Can Do GmbH unverzüglich schriftlich melden und dabei angeben, wie und unter welchen Umständen der Fehler bzw. der Mangel auftritt und die Can Do GmbH bei der Fehlersuche aktiv unterstützen.</p>	<p>The customer shall immediately notify Can Do GmbH in writing of any errors in the services covered by the contract and indicate how and under what circumstances the error or defect occurs and actively support Can Do GmbH in the search for the error.</p>
<p>Im Übrigen und soweit nicht in der Bestellung anders vereinbart, schuldet die Can Do GmbH keine weiteren Leistungen. Insbesondere ist die Can Do GmbH nicht zur Erbringung von vor Ort Installations-, Einrichtungs-, Beratungs-, Anpassungs- und / oder Schulungsleistungen sowie zur Erstellung und Überlassung von Individualprogrammierungen bzw. von Zusatzprogrammen verpflichtet.</p>	<p>In all other respects and unless otherwise agreed in the order, Can Do GmbH shall not owe any further services. In particular, Can Do GmbH is not obliged to provide onsite installation, setup, consulting, adaptation and/or training services or to create and provide individual programming or additional programs.</p>
<p>Die Can Do GmbH räumt dem Kunden für die Laufzeit der vereinbarten Nutzung das entgeltliche, nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare Recht ein, auf die Can Do Software auf dem Server der Can Do GmbH über das Internet zuzugreifen und mittels Webrowsers die mit der Can Do Software verbundenen Funktionalitäten nach Maßgabe dieser EULA zu nutzen. Darüberhinausgehende Rechte, insbesondere an der Software erhält der Kunde nicht. Eine Überlassung der Software an den Kunden erfolgt nicht.</p>	<p>For the duration of the agreed use, Can Do GmbH grants the Customer the non-exclusive, non-transferable, non-sublicensable right to access the Can Do Software on the server of Can Do GmbH via the Internet and to use the functionalities associated with the Can Do Software in accordance with this EULA via web browsers for a fee. The customer does not receive any further rights, in particular to the software. The software is not transferred to the customer.</p>
<p>Der Kunde ist nicht berechtigt, die Can Do Software über die nach Maßgabe dieses Vertrages erlaubte Nutzung hinaus zu nutzen oder sie Dritten zugänglich zu machen. Insbesondere ist es dem Kunden nicht gestattet, den Online-Service oder Teile davon, zu vervielfältigen, zu veräußern oder zeitlich begrenzt zu überlassen, vor allem nicht zu vermieten oder zu verleihen.</p>	<p>The customer is not entitled to use the Can Do Software beyond the use permitted under this contract or to make it accessible to third parties. In particular, the customer is not permitted to duplicate, sell or temporarily transfer the online service or parts thereof, and above all not to rent or lend it out.</p>
<p>Der Kunde darf die Can Do Software nur für seine eigenen geschäftlichen Tätigkeiten durch eigenes Personal und/oder beauftragte Dritte nutzen, die die Can Do Software für ihn nutzen („berechtigte Nutzer“). Der Kunde stellt sicher, dass die berechtigten Nutzer die Can Do Software nur im Rahmen und gemäß dieser EULA nutzen.</p>	<p>The customer may only use the Can Do Software for his own business activities by his own personnel and/or commissioned third parties who use the Can Do Software for him ("authorised users"). The Customer shall ensure that the Authorised Users</p>

End User Licence Agreement (EULA) Can Do (Can Do Software) Service

	use the Can Do Software only within the scope of and in accordance with this EULA.
Der Kunde wird die Can Do Software in keiner Weise missbräuchlich nutzen oder nutzen lassen, insbesondere keine rechtswidrigen Inhalte übermitteln. Der Kunde wird auch jeden Versuch unterlassen, selbst oder durch nicht autorisierte Dritte Informationen oder Daten unbefugt abzurufen oder in Programme, die von der Can Do GmbH betrieben werden, einzugreifen oder eingreifen zu lassen oder in Datennetze der Can Do GmbH unbefugt einzudringen.	The customer will not misuse the Can Do Software in any way or have it misused, in particular will not transmit any illegal content. The customer will also refrain from any attempt to retrieve information or data unauthorized by himself or by unauthorized third parties or to interfere or allow interference in programs operated by Can Do GmbH or to penetrate data networks of Can Do GmbH unauthorized.
Bei der Nutzung der Can Do Software sowie der vertragsgegenständlichen Leistungen wird der Kunde alle anwendbaren Gesetze und sonstigen Rechtsvorschriften beachten. Dem Kunden ist es insbesondere untersagt, Daten oder Inhalte einzustellen, die gegen Rechtsvorschriften verstoßen, die fremde Schutz- oder Urheberrechte oder sonstige Rechte Dritter verletzen. Der Kunde ist für die von ihm bereitgestellten Daten und Inhalte selbst verantwortlich. Die Can Do GmbH überprüft die Inhalte weder auf ihre Rechtmäßigkeit noch auf ihre Richtigkeit hin.	When using the Can Do Software as well as the contractual services, the customer will observe all applicable laws and other legal provisions. In particular, the customer is prohibited from uploading data or content that violates legal regulations, infringes third-party property rights or copyrights or other rights of third parties. The customer is responsible for the data and content provided by him. Can Do GmbH does not check the content for legality or accuracy.
Der Kunde stellt die Can Do GmbH von sämtlichen Ansprüchen Dritter frei, die auf einer rechtswidrigen Verwendung der Can Do Software durch ihn beruhen oder mit seiner Billigung erfolgen oder die sich insbesondere aus datenschutzrechtlichen, urheberrechtlichen oder sonstigen rechtlichen Streitigkeiten ergeben, die mit der Nutzung der Can Do Software verbunden sind. Erkennt der Kunde oder muss er erkennen, dass ein solcher Verstoß droht, besteht die Pflicht zur unverzüglichen Unterrichtung der Can Do GmbH.	The customer shall indemnify Can Do GmbH against all claims by third parties which are based on an unlawful use of the Can Do Software by him or which are made with his approval or which arise in particular from data protection, copyright or other legal disputes connected with the use of the Can Do Software. If the customer recognises or must recognise that such an infringement is imminent, Can Do GmbH is obliged to be informed immediately.
Der Kunde wird die ihm bzw. den Nutzern zugeordneten Nutzungs- und Zugangsberechtigungen sowie Identifikations- und Authentifikations-Sicherungen vor dem Zugriff durch Dritte schützen und nicht an unberechtigte Nutzer weitergeben. Sobald der Kunde Anzeichen dafür hat, dass die Nutzungs- und Zugangsberechtigungen von einem Dritten unrechtmäßig erlangt wurden oder missbraucht werden könnten, ist der Kunde wegen Schadensminderungszwecken verpflichtet, die Can Do GmbH umgehend hiervon zu informieren.	The customer shall protect the usage and access authorisations assigned to him or to the users as well as identification and authentication backups against access by third parties and shall not pass them on to unauthorised users. As soon as the Customer has indications that the usage and access authorisations have been illegally obtained by a third party or could be misused, the Customer is obliged to inform Can Do GmbH immediately in order to mitigate the damage.
Für jeden Fall, in dem Kunde die Nutzung der Can Do Software durch Dritte schuldhaft ermöglicht, hat Kunde jeweils eine sofort fällige Vertragsstrafe in Höhe der zweifachen, vereinbarten Vergütung zu zahlen. Die Geltendmachung von Schadensersatz bleibt der Can Do GmbH vorbehalten. In diesem Fall wird die Vertragsstrafe auf den Schadensersatzanspruch angerechnet. Im Falle einer unberechtigten Nutzungsüberlassung hat der Kunde der Can Do GmbH auf Verlangen unverzüglich sämtliche Angaben zur Geltendmachung der Ansprüche gegen den Nutzer zu machen, insbesondere dessen Namen und Anschrift mitzuteilen.	For each case in which the customer culpably enables third parties to use the Can Do Software, the customer shall pay an immediately due contractual penalty in the amount of twice the agreed remuneration. Can Do GmbH reserves the right to claim damages. In this case, the contractual penalty shall be set off against the claim for damages. In the event of an unauthorized transfer of use, the customer must provide Can Do GmbH immediately upon request with all information required to assert claims against the user, in particular the user's name and address.
Wird die vertragsgemäße Nutzung der Can Do Software ohne Verschulden der Can Do GmbH durch Schutzrechte Dritter beeinträchtigt, so ist die Can Do GmbH berechtigt, die hierdurch betroffenen Leistungen zu verweigern. Die Can Do GmbH wird den Kunden hiervon unverzüglich unterrichten und ihm in geeigneter Weise den Zugriff auf seine Daten ermöglichen. Der Kunde ist in diesem Fall nicht zur Zahlung verpflichtet. Sonstige Ansprüche oder Rechte des Kunden bleiben unberührt.	If the contractual use of the Can Do Software is impaired through no fault of Can Do GmbH by the property rights of third parties, Can Do GmbH shall be entitled to refuse the services affected thereby. Can Do GmbH will inform the customer of this immediately and enable him to access his data in an appropriate manner. In this case the customer is not obliged to pay. Other claims or rights of the customer remain unaffected.
Der Kunde wird, die an die Can Do Software übermittelten Daten regelmäßig und gefahrenstprechend sichern und eigene Sicherungskopien erstellen, um bei Verlust der Daten und Informationen die Rekonstruktion derselben zu gewährleisten. Die Datensicherung innerhalb der Can Do Software erfolgt entsprechend dem Stand der Technik und unter angemessener Berücksichtigung technischer Risiken.	The Customer shall regularly back up the data transmitted to the Can Do Software in accordance with the risks involved and create its own backup copies in order to ensure reconstruction of the data and information in the event of loss. The data backup within the Can Do Software takes place according to the state of the art and with appropriate consideration of technical risks.

End User Licence Agreement (EULA) Can Do (Can Do Software) Service

Wenn konkrete Anhaltspunkte vorliegen, dass der Kunde gegen eine der in diesem Vertrag festgelegten wesentlichen Pflichten, die gesetzlichen Bestimmungen oder Rechte Dritter verstößt bzw. verstoßen hat, oder wenn die Can Do GmbH ein sonstiges berechtigtes Interesse hat, ist die Can Do GmbH berechtigt,

- die betroffenen Daten zu löschen, zu deaktivieren oder zu verändern;
- andere geeignete Maßnahmen zu ergreifen, wie die Verwarnung des Kunden
- den Zugang des Kunden zu der Can Do Software unverzüglich zu sperren;

Bei der Entscheidung über eine Maßnahme wird die Can Do GmbH berechnete Interessen des Kunden berücksichtigen, insbesondere wenn der Kunde den Verstoß nicht verschuldet hat. Die Can Do GmbH wird den Kunden in allen Fällen vor der Sperrung per Email unterrichten.

Der Zugang wird erst dann wiederhergestellt, wenn der Verstoß gegen die betroffene wesentliche Pflicht dauerhaft beseitigt bzw. die Wiederholungsgefahr ausgeräumt ist. Bei besonders schwerwiegenden oder wiederholten, schuldhaften Verstößen ist die Can Do GmbH berechtigt, den Zugang des Kunden zu der Can Do Software und zu deren Daten dauerhaft zu sperren.

If there are concrete indications that the customer is violating or has violated one of the essential obligations stipulated in this contract, the statutory provisions or the rights of third parties, or if Can Do GmbH has any other justified interest, Can Do GmbH shall be entitled,

- delete, deactivate or modify the data concerned;
- to take other appropriate measures, such as warning the customer
- immediately block the Customer's access to the Can Do Software;

When deciding on a measure, Can Do GmbH will consider the legitimate interests of the customer, especially if the customer is not to blame for the violation. Can Do GmbH will inform the customer in all cases before the blocking by email.

Access shall not be restored until the breach of the essential obligation concerned has been permanently remedied or the risk of recurrence eliminated. In the event of particularly serious or repeated culpable violations, Can Do GmbH is entitled to permanently block the customer's access to the Can Do Software and its data.

Die vereinbarte Vergütung sowie die Abrechnungsperiode für die vertraglichen Leistungen ergeben sich aus der Bestellung des Kunden. Alle genannten Vergütungen und Entgelte verstehen sich zzgl. der jeweils gültigen gesetzlichen Umsatzsteuer zum Zeitpunkt der Leistungserbringung.

Der Kunde zahlt die vertraglich vereinbarte Vergütung für die jeweilige Abrechnungsperiode im Voraus über den gewählten Zahlungsweg. Unabhängig vom gewählten Zahlungsweg hat der Kunde die zur Abrechnung Verfügung gestellten Daten sowie seine Kundendaten jederzeit auf dem aktuellsten Stand zu halten und die Can Do GmbH über Änderungen unverzüglich zu informieren.

Kommt der Kunde a) für zwei aufeinander folgende Abrechnungsperioden mit der Bezahlung der Vergütung bzw. eines nicht unerheblichen Teils der Vergütung oder b) in einem Zeitraum, der sich über mehr als zwei Abrechnungsperioden erstreckt, mit der Bezahlung des Entgeltes in Höhe eines Betrages, der das Entgelt für zwei Abrechnungsperioden erreicht, in Verzug, ist die Can Do GmbH berechtigt, den Vertrag ohne Einhaltung einer Frist zu kündigen. Die Geltendmachung weiterer Ansprüche wegen Zahlungsverzuges bleibt ausdrücklich vorbehalten.

The agreed remuneration as well as the accounting period for the contractual services result from the customer's order. All remuneration and fees stated are exclusive of the statutory value-added tax applicable at the time the service is rendered.

The customer shall pay the contractually agreed remuneration for the relevant billing period in advance using the chosen payment method. Irrespective of the chosen payment method, the customer must keep the data provided for billing purposes and his customer data up to date at all times and inform Can Do GmbH immediately of any changes.

If the customer a) defaults on payment of the remuneration or a significant part thereof for two consecutive accounting periods or b) defaults on payment of the remuneration in an amount equal to the remuneration for two accounting periods in a period extending over more than two accounting periods, Can Do GmbH shall be entitled to terminate the contract without notice. We expressly reserve the right to assert further claims due to delayed payment.

Die Can Do GmbH haftet bei Vorsatz und grober Fahrlässigkeit sowie bei Verletzungen des Produkthaftungsgesetz sowie für Schadensersatzansprüche aus der DSGVO für alle von ihr und ihren gesetzlichen Vertretern oder Erfüllungsgehilfen verursachten Schäden nach den gesetzlichen Vorschriften. In Fällen leichter Fahrlässigkeit haftet die Can Do GmbH nur, für von ihr sowie ihren gesetzlichen Vertretern oder Erfüllungsgehilfen verursachten Schäden aus der Verletzung einer wesentlichen Vertragspflicht. Wesentlich sind Vertragspflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht und auf deren Einhaltung der Kunde regelmäßig vertraut und vertrauen darf. In diesem Fall ist die Haftung auf den Ersatz des vorhersehbaren, typischerweise eintretenden Schadens begrenzt. Die Haftung der Can Do GmbH für indirekte Schäden und entgangenen Gewinn ist ausgeschlossen. Die verschuldensunabhängige Haftung von die Can Do GmbH auf Schadensersatz (§ 536 a Abs.1 BGB) für bei Vertragsschluss vorhandene Mängel ist ausgeschlossen.

Can Do GmbH is liable in case of intent and gross negligence as well as in case of violations of the product liability law as well as for claims for damages arising from the GDPR for all damages caused by Can Do GmbH and its legal representatives or vicarious agents according to the legal regulations. In cases of slight negligence, Can Do GmbH shall only be liable for damages caused by it or its legal representatives or vicarious agents as a result of the breach of a essential contractual obligation. Essential are contractual obligations, the fulfilment of which is essential for the proper execution of the contract and on the observance of which the customer regularly relies and may rely. In this case the liability is limited to the replacement of the foreseeable, typically occurring damage. The liability of Can Do GmbH for indirect damages and loss of profit is excluded. The liability of Can Do GmbH for damages (§ 536 a Abs.1 BGB) for defects existing at the time of conclusion of the contract is excluded.

End User Licence Agreement (EULA) Can Do (Can Do Software) Service

<p>Die Can Do GmbH verarbeitet oder nutzt im Rahmen der Erbringung der Leistungen über die Speicherung von Daten durch den Kunden in der Can Do Software hinaus in der Regel keine personenbezogenen Daten des Kunden. Die Can Do GmbH erhebt lediglich anonymisierte Nutzungsstatistiken und Fehlerberichte. Soweit aber dennoch personenbezogene Daten in der Can Do Software abgelegt werden, ist Grundlage der Datenverarbeitung durch die Can Do GmbH die im Anhang zu diesen Bedingungen beigefügte Vereinbarung zur Auftragsverarbeitung („AVV“), die durch Annahme dieser EULA ausdrücklich zwischen den Parteien vereinbart wird. Erhebt, verarbeitet oder nutzt der Kunde personenbezogene Daten, so steht er dafür ein, dass er dazu nach den anwendbaren, insbesondere datenschutzrechtlichen Bestimmungen berechtigt ist und stellt im Falle eines Verstoßes der Can Do GmbH von Ansprüchen Dritter frei.</p>	<p>In addition to the storage of data by the customer in the Can Do Software, Can Do GmbH generally does not collect, process or use any personal data of the customer within the scope of providing the services. Can Do GmbH only collects anonymized usage statistics and bug reports. If, however, personal data is nevertheless stored in the Can Do Software, the basis for data processing by Can Do GmbH is the data processing agreement (“DPA”) attached as an annex to these Terms and Conditions, which is expressly agreed between the parties by acceptance of this EULA.</p> <p>If the customer collects, processes or uses personal data, he shall be responsible for ensuring that he is entitled to do so in accordance with the applicable, in particular data protection regulations, and shall indemnify Can Do GmbH against claims by third parties in the event of a breach.</p>
<p>Die Can Do GmbH ist von der Verpflichtung zur Leistung aus diesem Vertrag befreit, wenn und soweit die Nichterfüllung von Leistungen auf das Eintreten von Umständen höherer Gewalt nach Vertragsabschluss zurückzuführen ist. Als Umstände höherer Gewalt gelten zum Beispiel Krieg, Streiks, Unruhen, Enteignungen, wesentliche Rechtsänderungen, Sturm, Überschwemmungen und sonstige Naturkatastrophen sowie sonstige von der Can Do GmbH nicht zu vertretende Umstände, insbesondere Wassereintritte, Stromausfälle und Unterbrechungen oder Zerstörung datenführender Leitungen. Jede Vertragspartei hat die andere Vertragspartei über den Eintritt eines Falles von höherer Gewalt unverzüglich und in schriftlicher Form in Kenntnis zu setzen.</p>	<p>Can Do GmbH is released from the obligation to perform under this contract if and to the extent that the non-performance of services is due to the occurrence of circumstances of force majeure after conclusion of the contract. Circumstances of force majeure include war, strikes, riots, expropriations, major legal changes, storms, floods and other natural disasters as well as other circumstances for which Can Do GmbH is not responsible, in particular water intrusions, power failures and interruptions or destruction of data-carrying lines. Each Contracting Party shall immediately inform the other Contracting Party in writing of the occurrence of any case of force majeure.</p>
<p>Die Vertragsparteien verpflichten sich, Betriebs- und Geschäftsgeheimnisse, die sie - einschließlich ihrer Erfüllungsgehilfen - anlässlich der Vertragsanbahnung oder der Vertragserfüllung erlangt haben, vertraulich zu behandeln.</p>	<p>The contracting parties undertake to treat as confidential any trade and business secrets which they - including their vicarious agents - have acquired on the occasion of the initiation of the contract or the performance of the contract.</p>
<p>Der Vertrag wird über die in der Bestellung vereinbarte Vertragslaufzeit geschlossen (Mindestlaufzeit). Der Vertrag verlängert sich jeweils um den gleichen Zeitraum wie die Mindestvertragslaufzeit (Verlängerungslaufzeit), wenn nicht eine der Vertragsparteien den Vertrag vor Ende der Mindestlaufzeit oder der jeweiligen Verlängerungslaufzeit kündigt.</p>	<p>The contract is concluded for the term agreed in the order (minimum term). The contract shall be extended by the same period as the minimum contract period (extension period) unless one of the parties terminates the contract before the end of the minimum contract period or the respective extension period.</p>
<p>Änderungen oder Ergänzungen der Vereinbarungen zwischen den Parteien bedürfen der Textform.</p>	<p>Amendments or supplements to the agreements between the parties must be made in writing.</p>
<p>Im Falle der Unwirksamkeit einer oder mehrerer Bestimmungen dieser EULA bleiben die übrigen Bestimmungen in Kraft. Die rechtsunwirksame Bestimmung in dem Sinn und Zweck des Vertragsverhältnisses entsprechend durch die Parteien einvernehmlich durch eine wirksame Bestimmung zu ersetzen, die in ihrer wirtschaftlichen Auswirkung derjenigen der unwirksamen Bestimmung so nahe kommt wie rechtlich möglich</p>	<p>In the event that one or more provisions of this EULA are or become invalid, the remaining provisions shall remain in force. to replace the legally ineffective provision in the sense and purpose of the contractual relationship by an effective provision which in its economic effect comes as close as legally possible to that of the ineffective provision, by mutual agreement between the parties</p>
<p>Auf diesen Vertrag findet das Recht der Bundesrepublik Deutschland unter Ausschluss des Übereinkommens der Vereinten Nationen über Verträge über den internationalen Warenkauf (CISG) und des deutschen Kollisionsrechts Anwendung.</p>	<p>The law of the Federal Republic of Germany shall apply to this contract to the exclusion of the United Nations Convention on Contracts for the International Sale of Goods (CISG) and the German conflict of laws provisions.</p>
<p>Soweit der Kunde nicht Verbraucher im Sinne von § 13 BGB ist, ist Gerichtsstand für alle Streitigkeiten aus diesem Vertrag einschließlich seiner Anhänge München. Dasselbe gilt, wenn der Kunde keinen allgemeinen Gerichtsstand in Deutschland hat oder Wohnsitz oder gewöhnlicher Aufenthalt im Zeitpunkt der Klageerhebung nicht bekannt sind.</p>	<p>If the customer is not a consumer within the meaning of § 13 BGB (German Civil Code), the place of jurisdiction for all disputes arising from this contract including its appendices shall be Munich. The same applies if the customer does not have a general place of jurisdiction in Germany or if his place of residence or habitual abode is not known at the time the action is filed.</p>
<p>Vertragsprache ist Deutsch. Diese EULA sind in deutscher und englischer Fassung erhältlich. Für die Auslegung einzelner Regelungen</p>	<p>The contract language is German. This EULA is available in German and English. For the interpretation of individual</p>

End User Licence Agreement (EULA) Can Do (Can Do Software) Service

und/oder bei Widersprüchen zwischen den Sprachfassungen ist die deutsche Sprachfassung allein maßgeblich und verbindlich.

regulations and/or in the event of contradictions between the language versions, the German language version alone shall be authoritative and binding.

Auftragsverarbeitungsvereinbarung (AVV) Can Do (Can Do Software) Service

1. Gegenstand und Dauer des Auftrags

- (1) Der Gegenstand des Auftrags ergibt sich aus dem Hauptvertrag und/oder dem Service und Wartungsvertrag, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).
- (2) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

- (1) Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber werden nachfolgend konkretisiert:

Der Auftragnehmer betreibt eine Online-Projektmanagement-Lösung, welche der Auftraggeber für die Planung und Steuerung seiner Projekte einsetzen wird. Bestandteil dieser Projektmanagement-Lösung sind das Ressourcenmanagement, die Personaleinsatzplanung im Rahmen der Projekte, das Controlling der Projekte sowie Risikomanagement und Berichtswesen inkl. Exportfunktion.

Im Rahmen des Multiprojektmanagements werden teilnehmerbezogene Daten auch projektübergreifend miteinander verknüpft.

Projektteilnehmer werden als Ressource angelegt und verwaltet. Projektleitung, Teilnehmer und deren Führungskräfte erhalten personengebunden Zugang zu der Plattform mit der Möglichkeit, jeweils individuell bzw. über Rollen festgelegte Tätigkeiten durchzuführen und die hierfür notwendigen personenbezogenen Daten zu sehen bzw. zu ändern.

- (2) 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 Artt. 44 ff. DS-GVO erfüllt sind.

- (3) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Personenstammdaten
- Kontaktdaten
- Lage und Dauer der Erholungsurlaube der Projektbeteiligten
- Lage und Dauer sonstiger Abwesenheiten (z. B. Arbeitsunfähigkeit) der Projektbeteiligten
- Planungsdaten
- Informationen zu tatsächlich geleisteten Aufwänden, bezogen auf einzelne Projektaktivitäten
- Sämtliche textuellen Informationen, welche durch die Nutzer erfasst werden

- (4) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Ansprechpartner von Dienstleistern des Auftraggebers
- Beschäftigte i. S. d. § 26 Abs. 8 BDSG des Auftraggebers
- Unter Umständen (nur sofern nicht vermeidbar) Nutzer von Wohneinheiten für welche der Auftraggeber Verbrauchsmessungen und andere Dienstleistungen erbringt

3. Technisch-organisatorische Maßnahmen

- (1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der

Auftragsverarbeitungsvereinbarung (AVV) in Englisch Can Do (Can Do Software) Service

konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

- (2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].
- (3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

- (1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
- (2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) Schriftliche Benennung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt, sofern eine entsprechende gesetzliche Verpflichtung besteht. Ist ein Datenschutzbeauftragter benannt, werden dessen Kontaktdaten dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
- b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].
- d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen
- g)

Auftragsverarbeitungsvereinbarung (AVV) in Englisch Can Do (Can Do Software) Service

Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

- h) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- i) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

- (1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
- (2) Der Auftragnehmer darf ohne Zustimmung des Auftraggebers keine Unterauftragnehmer (weitere Auftragsverarbeiter) beauftragen.

7. Kontrollrechte des Auftraggebers

- (1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
- (2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
- (3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch
 - die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
 - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
 - aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
 - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).
- (4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
- b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

Auftragsverarbeitungsvereinbarung (AVV) in Englisch Can Do (Can Do Software) Service

- e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

9. Weisungsbefugnis des Auftraggebers

- (1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).
- (2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

- (1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
- (2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
- (3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Anhang – Technisch-organisatorische Maßnahmen Can Do zur Wahrung der Datensicherheit gemäß Art. 32 EU-DSGVO

Die Can Do GmbH berücksichtigt zahlreiche technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit in der Verarbeitung personenbezogener Daten. Wir bekennen uns zu den datenschutzrechtlichen Vorschriften der EU-DSGVO (Europäische Datenschutzgrundverordnung) und des BDSG (Bundesdatenschutzgesetz), wie sie seit dem 25. Mai 2018 anzuwenden sind. Die folgende Übersicht führt die TOMs an, die zur Sicherstellung der IT-Sicherheit in unserem Unternehmen im Einsatz sind.

Eine hervorzuhebende Stellung nehmen in diesem Kontext unsere beiden zentralen externen Auftragsdatenverarbeiter HubSpot und Amazon Web Services (AWS) ein:

1. HubSpot als zentrales CRM-Tool

Unser Unternehmen bietet Kunden eine Projektmanagement Software zur professionellen Planung von Vorhaben und Ressourcen an. Für die effizienten Abwicklung sämtlicher unternehmensinterner Geschäftsprozesse kommt hierfür in erster Linie die Inbound-Marketing Plattform HubSpot im Rahmen einer Auftragsverarbeitung gem. Art. 29 DSGVO zum Einsatz. HubSpot ist ein webbasiertes Cloudcomputing Tool für Vertrieb, Marketing und Kundenservice. Die Verarbeitungen von personenbezogener Kundendaten findet entsprechend unter anderem über HubSpot statt. Rechtsgrundlage für die Nutzung von HubSpot ist unser berechtigtes Interesse zur effizienten Abwicklung unserer Geschäftsprozesse und der Verfolgung unserer Geschäftsinteressen, gem. Art. 6 Abs. 1 lit. f DSGVO.

Wir haben einen Auftragsverarbeitungsvertrag (DPA) mit HubSpot abgeschlossen. In diesem garantiert HubSpot den ordnungsgemäßen Einsatz der in Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Die konkreten, von HubSpot berücksichtigten Sicherheitsmaßnahmen können der Anlage 2 der DPA von HubSpot entnommen werden: <https://legal.hubspot.com/de/dpa>

Auftragsverarbeitungsvereinbarung (AVV) in Englisch Can Do (Can Do Software) Service

2. Amazon Web Services (AWS) als zentraler Webhoster

Die Anwendungs- und Benutzerdaten unserer Kunden werden mit Hilfe verschiedener AWS-Dienste (Amazon Web Services) wie Computing, Storage, Networking usw. verwaltet und verarbeitet. Der Betrieb wird im Amazon Rechenzentrum in Frankfurt (EU Central/Frankfurt am Main) durchgeführt. Die Redundanzsysteme durch Amazon werden in EU Central – 1A und 1B geführt. Amazon sichert zu, dass alle Daten innerhalb des Europäischen Wirtschaftsraum verarbeitet und somit die Anforderungen der EU-DSGVO zu jedem Zeitpunkt der Verarbeitung eingehalten werden.

Mit AWS wurde ebenfalls ein Auftragsvertragsvertrag gem. Art. 29 DSGVO abgeschlossen, der den Anbieter u.a. zum Einsatz adäquater technischer und organisatorischer Maßnahmen verpflichtet. Unser Partner AWS hat folgende Zertifizierungen im Hinblick auf die Einhaltung gängiger IT-Standards:

<https://aws.amazon.com/de/compliance/programs/>

In den Räumlichkeiten der Can Do GmbH kommen ebenfalls Datenverarbeitungsanlagen zum Einsatz. Diese werden für die Verarbeitung von personenbezogenen bzw. Kundendaten ausschließlich anlassbezogen eingesetzt. Derartige Verarbeitungszwecke sind beispielsweise das Anlegen neuer Aufträge, die Überwachung des ordnungsgemäßen Geschäftsbetriebs, die Überprüfung auf Korrektheit der Daten, oder die Korrektur von Daten bei notwendigen Änderungen. Die Datenverarbeitung erfolgt stets in Übereinstimmung mit den jeweiligen Vertragsvereinbarungen.

In keinem Fall werden personenbezogene Daten dauerhaft auf unseren Geräten gespeichert.

3. Übersicht der TOMs gemäß §64 BDSG:

In unseren Räumlichkeiten bzw. auf den von uns eingesetzten Systemen werden insbesondere die folgenden technischen und organisatorischen Maßnahmen (TOMs) zur Wahrung der Sicherheit in der Verarbeitung personenbezogener Daten berücksichtigt:

4. Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte Zugang zu Verarbeitungsanlagen erhalten, mit denen die Verarbeitung durchgeführt wird:

- Einsatz eines Alarmanlagen Systems
- Einsatz von abschließbaren Serverschränke
- Einsatz von Sicherheitsschlössern

5. Datenträgerkontrolle

Maßnahmen, die verhindern, dass Unbefugte Datenträger lesen, kopieren, verändern oder löschen können.

- Sichere Aufbewahrung von Datenträgern
- Einrichtungen von Standleitungen beziehungsweise VPN-Tunneln
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Verschlüsselung von (mobilen) Datenträgern
- Ordnungsgemäße Vernichtung von Datenträgern
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Protokollierung der Vernichtung

6. Speicherkontrolle

Maßnahmen, die verhindern, dass Unbefugte von gespeicherten personenbezogenen Daten Kenntnis nehmen sowie diese eingeben, verändern und löschen können.

- Festlegung von Berechtigungen in den IT-Systemen
- Einsatz eines Berechtigungskonzepts das die Berechtigungen für lesen, löschen und ändern differenziert und regelt
- Einsatz eines Berechtigungskonzepts das Daten, Anwendungen und Administration der Betriebssysteme differenziert und regelt
- Verwaltung der Berechtigungen durch Systemadministratoren
- Die Anzahl der Administratoren wird auf das „Notwendigste“ reduziert
- Einsatz einer Passwort Richtlinie
- Einsatz von Zugriff-Protokollen auf Anwendungen

7. Benutzerkontrolle

Maßnahmen, die verhindern, dass Unbefugte automatisierte Verarbeitungssysteme mit Hilfe von Datenübertragung nutzen können.

- Festlegung zugangsberechtigter Mitarbeiter
- Einsatz von Benutzerprofilen mit unterschiedlichen Zugriffsrechten
- Einsatz eines Passwortmanagements
- Zugriff nur nach Authentifikation mit Benutzername/Passwort
- Regelmäßige Kontrolle von Berechtigungen
- Sperrung von Berechtigungen ausscheidender Mitarbeiter
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von fortlaufend aktualisierter Verschlüsselungs-Technologie
- Einsatz von fortlaufend aktualisierter Anti-Viren-Software

8. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

- Festlegung von Berechtigungen in den IT-Systemen
- Einsatz eines Berechtigungskonzepts das die Berechtigungen für lesen, löschen und ändern differenziert und regelt
- Einsatz eines Berechtigungskonzepts das Daten, Anwendungen und Administration der Betriebssysteme differenziert und regelt
- Verwaltung der Berechtigungen durch Systemadministratoren
- Die Anzahl der Administratoren wird auf das „Notwendigste“ reduziert
- Einsatz von Zugriff-Protokollen auf Anwendungen
- Einsatz einer Passwortrichtlinie inkl. Passwortlänge und Passwortwechsel

9. Übertragungskontrolle

Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

- Einsatz von Standleitungen beziehungsweise Verschlüsselungs-Technologie
- Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung beziehungsweise vereinbarter Löschfristen

10. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem eingegeben oder verändert worden sind.

- Eingabeprotokollierung mit eindeutiger Benutzerzuweisung in unserem CRM-System

11. Transportkontrolle

Maßnahmen, die gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

- Einsatz von Standleitungen beziehungsweise Verschlüsselungs-Technologie
- Ausschließlicher Einsatz von Auftragsverarbeitern mit angemessenen technischen und organisatorischen Maßnahmen

12. Wiederherstellbarkeit

Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störfall wiederhergestellt werden können.

- Einsatz eines Backup- & Recoverykonzepts
- Regelmäßiges Testen der Datenwiederherstellung
- Einsatz eines Notfallplans für den Störfall

13. Zuverlässigkeit

Maßnahmen, die gewährleisten, dass alle Funktionen der Systeme zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

- Einsatz von unabhängig voneinander funktionierenden Systemen
- Einsatz von IT-sicherheitskonformen Cloud Computing Prozessen
- Automatisierte Benachrichtigung im Fall von Fehlfunktionen der Systeme
- Einsatz von fortlaufend aktualisierter Anti-Viren-Software

14. Datenintegrität

Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden.

- Einsatz eines Backup- & Recoverykonzepts

15. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend unseren Weisungen verarbeitet werden.

- Ausschließlicher Einsatz von Auftragsverarbeitern mit angemessenen technischen und organisatorischen Maßnahmen
- Regelmäßige Überprüfung und Evaluierung der externen Dienstleister, die im Rahmen einer Auftragsverarbeitung personenbezogene Daten verarbeiten.

16. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen physische Zerstörung oder Verlust geschützt sind.

- Einsatz von Geräten zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Einsatz von Feuerlöschgeräten in Serverräumen
- Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
- Einsatz eines Notfallplans für den Fall des Datenverlusts

17. Trennbarkeit

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden.

- Trennung von Anwendungen und Speicherort der Daten
- Einsatz eines CRM-Systems, welches das gleichzeitige Arbeiten an Daten aus unterschiedlichen Beständen nicht vorsieht.

Auftragsverarbeitungsvereinbarung (AVV) in Englisch Can Do (Can Do Software) Service

1. Subject and duration of the order

- (1) The subject matter of the order results from the main contract and/or the service and maintenance contract referred to here (hereinafter referred to as service agreement).
- (2) The duration of this contract (term) corresponds to the term of the service agreement.

2. Concretization of the order content

- (1) The nature and purpose of the processing of personal data by the contractor for the client are specified below:

The contractor operates an online project management solution, which the client will use for planning and controlling his projects. This project management solution includes resource management, personnel deployment planning within the projects, project controlling, risk management and reporting, including an export function.

Within the framework of multi-project management, participant-related data is also linked across projects.

Project participants are created and managed as resources. Project managers, participants and their executives receive personalized access to the platform with the possibility to carry out activities defined individually or via roles and to view or change the personal data required for this.
- (2) The provision of the contractually agreed data processing takes place exclusively in a member state of the European Union or in another state that is a party to the Agreement on the European Economic Area. Any relocation to a third country requires the prior consent of the customer and may only take place if the special conditions of Art. 44 ff. DS-GVO are fulfilled.
- (3) The following types/categories of data are subject to the processing of personal data:

Person master data

contact details

Location and duration of the recreational vacations of the project participants

Location and duration of other absences (e.g. incapacity to work) of project participants

Planning data

Information on actual expenses, related to individual project activities

All textual information collected by the user

- (4) The categories of data subjects covered by the processing operation:
 - Contact person of service providers of the client
 - Employees within the meaning of § 26 para. 8 BDSG of the client
 - Under certain circumstances (only if unavoidable) users of residential units for which the client provides consumption measurements and other services

3. Technical-organizational measures

- (1) The Contractor shall document the implementation of the technical and organizational measures described and required in the run-up to the award of the contract prior to the start of processing, in particular with regard to the concrete execution of the contract, and shall hand them over to the Client for inspection. If accepted by the customer, the documented measures will become the basis of the order. Insofar as the examination/audit of the client reveals a need for adjustment, this shall be implemented by mutual agreement.
- (2) The contractor must provide the security in accordance with Art. 28 para. 3 lit. c, 32 DS-GVO, in particular in connection with Art. 5 para. 1, para. 2 DS-GVO. Overall, the measures to be taken are data security measures and to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. The state of the art, the implementation costs and the nature, scope and purposes

Auftragsverarbeitungsvereinbarung (AVV) in Englisch Can Do (Can Do Software) Service

of the processing as well as the varying probability of occurrence and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 (1) DS-GVO must be taken into account [details in Annex 1].

- (3) The technical and organizational measures are subject to technical progress and further development. In this respect the contractor is permitted to implement alternative adequate measures. In doing so, the safety level of the specified measures may not be undercut. Significant changes must be documented.

4. Correction, restriction and deletion of data

- (1) The Contractor may not correct, delete or restrict the processing of the data processed on behalf of the Client, but only after documented instructions from the Client. Insofar as a person concerned contacts the contractor directly in this respect, the contractor shall forward this request to the customer without delay.
- (2) As far as included in the scope of services, the deletion concept, right to be forgotten, correction, data portability and information are to be ensured directly by the contractor according to documented instructions of the customer.

5. Quality assurance and other obligations of the contractor

In addition to complying with the provisions of this contract, the contractor has statutory obligations pursuant to Art. 28 to 33 DS-GVO; in this respect, the contractor guarantees in particular compliance with the following requirements:

- a. Written appointment of a data protection officer who carries out his or her activities in accordance with Art. 38 and 39 DS-GVO, provided that there is a corresponding legal obligation. If a data protection officer has been appointed, his or her contact details will be communicated to the client for the purpose of direct contact. The client will be informed immediately of any change in the data protection officer.
- b. The maintenance of confidentiality in accordance with Art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 DS-GVO. In carrying out the work, the contractor shall only use employees who are bound to confidentiality and who have been previously familiarized with the provisions on data protection relevant to them. The contractor and any person subordinate to the contractor who has access to personal data may process such data exclusively in accordance with the instructions of the customer, including the powers granted in this agreement, unless they are legally obliged to process such data.
- c. The implementation of and compliance with all technical and organizational measures required for this order in accordance with Art. 28 para. 3 sentence 2 letter c, 32 DS-GVO [details in Annex 1].
- d. The Customer and the Contractor shall, upon request, cooperate with the Supervisory Authority in the performance of its tasks.
- e. The immediate information of the client about control actions and measures of the supervisory authority, as far as they relate to this contract. This shall also apply if a competent authority investigates in the course of administrative or criminal proceedings relating to the processing of personal data in connection with the processing of the contract at the contractor.
- f. If the customer, for his part, is subject to an inspection by the supervisory authority, administrative offence or criminal proceedings, a liability claim by a data subject or third party or any other claim in connection with the processing of the order with the contractor, the contractor shall assist him to the best of his ability.
- g. The Contractor shall regularly check the internal processes and the technical and organizational measures to ensure that the processing in its area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the protection of the rights of the data subject is guaranteed.
- h. Verifiability of the technical and organizational measures taken vis-à-vis the customer within the scope of his powers of control according to clause 7 of this contract.

6. Subcontracting relationships

- (1) Subcontracting relationships within the meaning of this provision are understood to be those services which are directly related to the provision of the main service. This does not include ancillary services which the Contractor

Auftragsverarbeitungsvereinbarung (AVV) in Englisch Can Do (Can Do Software) Service
uses e.g. as telecommunication services, postal/transport services, maintenance and user service or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the Contractor is obliged to take appropriate and legally compliant contractual agreements and control measures to ensure data protection and data security of the Customer's data, even in the case of outsourced ancillary services.

(2) The Contractor may not commission subcontractors (further processors) without the Customer's consent.

7. Control rights of the client

- (1) The customer has the right to carry out inspections in consultation with the contractor or to have them carried out by inspectors to be named in individual cases. He shall have the right to convince himself of the contractor's compliance with this agreement in his business operations by means of spot checks, which as a rule must be notified in good time.
- (2) The contractor shall ensure that the customer can satisfy himself that the contractor's obligations under Art. 28 DS-GVO have been met. The contractor undertakes to provide the customer on request with the necessary information and in particular to provide evidence of the implementation of the technical and organizational measures.
- (3) The proof of such measures, which do not only concern the specific order, can be provided by
 - compliance with approved rules of conduct in accordance with Art. 40 DS-GVO;
 - certification in accordance with an approved certification procedure pursuant to Art. 42 DS-GVO;
 - current certificates, reports or report extracts from independent bodies (e.g. auditors, revision, data protection officer, IT security department, data protection auditors, quality auditors);
 - a suitable certification through IT security or data protection audit (e.g. according to BSI basic protection).
- (4) The Contractor may assert a claim for remuneration for enabling the Client to carry out checks.

8. Notification in case of violations by the contractor

The Contractor shall assist the Principal in complying with the obligations regarding the security of personal data as set out in Articles 32 to 36 of the DS-GVO, reporting obligations in the event of data breaches, data protection impact assessments and prior consultations. This includes, among other things

- a. ensuring an adequate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing as well as the predicted probability and severity of a possible breach of rights due to security vulnerabilities and allow for the immediate detection of relevant breach events
- b. the obligation to report violations of personal data immediately to the client
- c. the obligation to support the client within the scope of his duty to inform the person concerned and to provide him with all relevant information in this context without delay
- d. support of the client for its data protection impact assessment
- e. the support of the client in the context of prior consultations with the supervisory authority

9. Authority of the client

- (1) Verbal instructions are confirmed by the client immediately (at least in text form).
- (2) The Contractor must inform the Client immediately if he believes that an instruction violates data protection regulations. Contractor shall be entitled to suspend the execution of the relevant instruction until it is confirmed or amended by Customer.

10. Deletion and return of personal data

- (1) No copies or duplicates of the data will be made without the knowledge of the client. Excluded from this are back-up copies, insofar as they are necessary to ensure proper data processing, as well as data which is required in order to comply with statutory storage obligations.

Auftragsverarbeitungsvereinbarung (AVV) in Englisch Can Do (Can Do Software) Service

- (2) Upon completion of the contractually agreed work or earlier upon request by the Customer - at the latest upon termination of the service agreement - the Contractor shall hand over to the Customer all documents, processing and usage results and data stocks that have come into its possession and are related to the contractual relationship, or destroy them in accordance with data protection laws upon prior consent. The same applies to test and reject material. The protocol of the deletion must be presented on request.

- (3) Documentation that serves as proof of the orderly and proper processing of data must be kept by the contractor in accordance with the respective retention periods beyond the end of the contract. He can hand them over to the customer at the end of the contract to relieve him.

Auftragsverarbeitungsvereinbarung (AVV) in Englisch Can Do (Can Do Software) Service

Appendix - Technical-organizational measures Can Do to ensure data security according to Art. 32 EU-DSGVO

(Status: July 2020)

Can Do GmbH takes numerous technical and organizational measures to ensure security in the processing of personal data. We are committed to the data protection regulations of the EU-DSGVO (European Data Protection Basic Regulation) and the BDSG (Federal Data Protection Act), as they have been applicable since May 25, 2018. The following overview lists the TOMs that are used to ensure IT security in our company.

In this context, our two centralized external order data processors HubSpot and Amazon Web Services (AWS) play an important role:

1. HubSpot as central CRM tool

Our company offers customers a project management software for professional planning of projects and resources. For the efficient handling of all internal business processes, we primarily use the inbound marketing platform HubSpot within the scope of order processing according to Art. 29 DSGVO. HubSpot is a web-based cloud computing tool for sales, marketing and customer service. Accordingly, the processing of personal customer data takes place via HubSpot, among other things. Legal basis for the use of HubSpot is our legitimate interest in the efficient handling of our business processes and the pursuit of our business interests, in accordance with Art. 6 para. 1 lit. f DSGVO.

We have a contract processing agreement (DPA) with HubSpot. In this contract HubSpot guarantees the proper use of the technical and organizational measures required in Art. 32 DSGVO. The specific security measures taken into account by HubSpot can be found in Appendix 2 of the DPA of HubSpot: <https://legal.hubspot.com/de/dpa>

2. Amazon Web Services (AWS) as central web host

Our customers' application and user data is managed and processed using various AWS (Amazon Web Services) services such as computing, storage, networking, etc. The operation is performed in the Amazon data center in Frankfurt (EU Central/Frankfurt am Main). The redundancy systems by Amazon are managed in EU Central - 1A and 1B. Amazon assures that all data is processed within the European Economic Area and thus the requirements of the EU-DSGVO are met at all times during processing.

An order processing contract was also concluded with AWS in accordance with Art. 29 DSGVO, which obliges the provider to use adequate technical and organizational measures, among other things. Our partner AWS has the following certifications with regard to compliance with common IT standards:

<https://aws.amazon.com/de/compliance/programs/>

The premises of Can Do GmbH are also equipped with data processing systems. These are used for the processing of personal or customer data exclusively for specific occasions. Such processing purposes are, for example, the creation of new orders, the monitoring of proper business operations, the checking of the correctness of data, or the correction of data in case of necessary changes. Data processing is always carried out in accordance with the respective contractual agreements.

Under no circumstances will personal data be permanently stored on our devices.

3. Overview of TOMs according to §64 BDSG:

On our premises or on the systems used by us, the following technical and organizational measures (TOMs) are particularly taken into account to ensure security in the processing of personal data:

4. Access control

Measures to prevent unauthorized persons from gaining access to processing equipment used for processing:

- Use of an alarm system
- Use of lockable server racks
- Use of security locks

5. Data medium control

Measures to prevent unauthorized persons from reading, copying, modifying or deleting data media.

Auftragsverarbeitungsvereinbarung (AVV) in Englisch Can Do (Can Do Software) Service

- Secure storage of data media
- Installation of dedicated lines or VPN tunnels
- Transfer of data in anonymized or pseudonymized form
- Encryption of (mobile) data media
- Proper destruction of data media
- Use of document shredders or service providers (if possible with data protection seal of approval)
- Logging of the destruction

6. Storage control

Measures to prevent unauthorized persons from taking note of stored personal data and from entering, changing and deleting it.

- Definition of authorizations in the IT systems
- Use of an authorization concept that differentiates and regulates the authorizations for read, delete and change
- Use of an authorization concept that differentiates and controls data, applications and administration of the operating systems
- Management of authorizations by system administrators
- The number of administrators is reduced to the "bare minimum"
- Use of a password policy
- Use of access protocols to applications

7. User control

Measures that prevent unauthorized persons from using automated processing systems by means of data transmission.

- Definition of employees with access rights
- Use of user profiles with different access rights
- Use of a password management system
- Access only after authentication with user name/password
- Regular control of authorizations
- Blocking of authorizations of departing employees
- Assignment of user profiles to IT systems
- Use of continuously updated encryption technology
- Use of continuously updated anti-virus software

8. Access control

Measures to ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation.

- Definition of authorizations in the IT systems
- Use of an authorization concept that differentiates and regulates the authorizations for read, delete and change
- Use of an authorization concept that differentiates and controls data, applications and administration of the operating systems
- Management of authorizations by system administrators
- The number of administrators is reduced to the "bare minimum"
- Use of access protocols to applications
- Use of a password policy including password length and password change

9. Transfer control

Measures to ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data transmission equipment.

- Use of dedicated lines or encryption technology
- Create an overview of regular retrieval and transmission processes
- Documentation of the recipients of data and the time periods of the planned transfer or agreed deletion periods

Auftragsverarbeitungsvereinbarung (AVV) in Englisch Can Do (Can Do Software) Service

10. Input control

Measures to ensure that it is possible to subsequently check and establish which personal data has been entered or modified, at what time and by whom.

- Input logging with clear user assignment in our CRM system

11. Transport control

Measures to ensure that the confidentiality and integrity of data is protected during the transmission of personal data and the transport of data carriers.

- Use of dedicated lines or encryption technology
- Exclusive use of contract processors with appropriate technical and organizational measures

12. Restorability

Measures to ensure that systems in use can be restored in the event of a fault.

- Use of a backup & recovery concept
- Regular testing of the data recovery
- Use of a contingency plan for the event of an incident

13. Reliability

Measures that ensure that all functions of the systems are available and that any malfunctions are reported.

- Use of independently functioning systems
- Use of IT security compliant cloud computing processes
- Automated notification in case of system malfunction
- Use of continuously updated anti-virus software

14. Data integrity

Measures to ensure that stored personal data is not damaged by system malfunction.

- Use of a backup & recovery concept

15. Order control

Measures to ensure that personal data processed by order are only processed according to our instructions.

- Exclusive use of contract processors with appropriate technical and organizational measures
- Regular review and evaluation of the external service providers who process personal data in the context of an order processing

16. Availability control

Measures to ensure that personal data is protected against physical destruction or loss.

- Use of devices for monitoring temperature and humidity in server rooms
- Use of fire extinguishing equipment in server rooms
- Storage of backups in a secure, outsourced location
- Use of a contingency plan in case of data loss

17. Separability

Measures to ensure that personal data collected for different purposes are processed separately.

- Separation of applications and data storage location
- Use of a CRM system that does not allow simultaneous work on data from different sources.