

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/software 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/software 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 Webbrowsers 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</p>	<p>The customer may only use the Can Do Software for his own business activities by his own personnel and/or commissioned</p>

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

<p>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>third parties who use the Can Do Software for him ("authorised users"). The Customer shall ensure that the Authorised Users use the Can Do Software only within the scope of and in accordance with this EULA.</p>
<p>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.</p>	<p>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.</p>
<p>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.</p>	<p>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.</p>
<p>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.</p>	<p>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.</p>
<p>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.</p>	<p>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.</p>
<p>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.</p>	<p>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.</p>
<p>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.</p>	<p>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.</p>
<p>Der Kunde wird, die an die Can Do Software übermittelten Daten regelmäßig und gefahrensprechend sichern und eigene Sicherungskopien erstellen, um bei Verlust der Daten und Informationen die Rekonstruktion derselben zu gewährleisten. Die</p>	<p>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</p>

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

<p>Datensicherung innerhalb der Can Do Software erfolgt entsprechend dem Stand der Technik und unter angemessener Berücksichtigung technischer Risiken.</p>	<p>backup within the Can Do Software takes place according to the state of the art and with appropriate consideration of technical risks.</p>
<p>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,</p> <ul style="list-style-type: none"> • 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; <p>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.</p> <p>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.</p>	<p>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,</p> <ul style="list-style-type: none"> • 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; <p>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.</p> <p>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.</p>
<p>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.</p> <p>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.</p> <p>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.</p>	<p>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.</p> <p>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.</p> <p>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.</p>
<p>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</p>	<p>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</p>

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

<p>verschuldensunabhängige Haftung von die Can Do GmbH auf Schadensersatz (§ 536 a Abs.1 BGB) für bei Vertragsschluss vorhandene Mängel ist ausgeschlossen.</p>	<p>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.</p>
<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 Wassereinträge, 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</p>

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

	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.
Vertragssprache ist Deutsch. Diese EULA sind in deutscher und englischer Fassung erhältlich. Für die Auslegung einzelner Regelungen und/oder bei Widersprüchen zwischen den Sprachfassungen ist die deutsche Sprachfassung allein maßgeblich und verbindlich.	The contract language is German. This EULA is available in German and English. For the interpretation of individual 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 Cloudvertrag und den EULA 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 sind konkret beschrieben in der Leistungsvereinbarung.
- (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) Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben.
- (4) Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben.

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 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. Artt. 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 Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
- b) Die Wahrung der Vertraulichkeit gemäß Artt. 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 Artt. 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 Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- g) 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.
- h) 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) Genehmigte Unterauftragnehmer sind in Anlage 3 zum Cloudvertrag aufgeführt.
- (3) 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,

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

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

- (1) 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
 - e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde
- (2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

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.

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

- (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

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen: Schlüssel, elektrische Türöffner, Alarmanlagen
- Zugangskontrolle
Keine unbefugte Systembenutzung: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zugriffskontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden: Mandantenfähigkeit;

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind: Protokollierung, Dokumentenmanagement;

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management;
- Incident-Response-Management.

AWS Security Standards (Amazon)

Capitalised terms not otherwise defined in this document have the meanings assigned to them in the Agreement.

1. Information Security Program. AWS will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorised access to the AWS Network, and (c) minimise security risks, including through risk assessment and regular testing. AWS will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

1.1 Network Security. The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats.

1.2 Physical Security

1.2.1 Physical Access Controls. Physical components of the AWS Network are housed in nondescript facilities (the "Facilities"). Physical barrier controls are used to prevent unauthorised entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorised employees or contractors while visiting the Facilities.

1.2.2 Limited Employee and Contractor Access. AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access

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

privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its Affiliates.

1.2.3 Physical Security Protections. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorised access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All

AWS GDPR Data Processing Addendum 9

physical access to the Facilities by employees and contractors is logged and routinely audited.

2. Continued Evaluation. AWS will conduct periodic reviews of the security of its AWS Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. AWS will continually evaluate the security of its AWS Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

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

1. Subject and duration of the contract

- (3) The subject matter of the order results from the Cloud-Agreement and the EULA to which reference is made here (hereinafter referred to as Service Agreement).
- (4) The duration of this contract (term) corresponds to the term of the Service Agreement.

2. Concretisation of the content of the contract

- (5) The nature and purpose of the processing of personal data by the Contractor for the Customer are specifically described in the Service Agreement.
- (6) The provision of the contractually agreed data processing takes place exclusively in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. Any relocation to a third country shall require the prior consent of the contracting authority and may take place only if the special conditions of Art. 44 et seq. of the GDPR are fulfilled.
- (7) The type of personal data used is described in the Service Agreement.
- (8) The categories of data subjects involved in the processing are specifically described in the Service Agreement.

3. Technical-organisational measures

- (4) The Contractor shall document the implementation of the technical and organisational measures set out and required prior to the award of the contract prior to commencement of processing, in particular with regard to the concrete execution of the contract and shall hand them over to the Customer for inspection. If accepted by the Customer, the documented measures become the basis of the order. If the inspection/audit of the Customer reveals a need for adjustment, this must be implemented by mutual agreement.
- (5) The Contractor shall provide the security pursuant to Art. 28 para. 3 lit. c, 32 GDPR, in particular in conjunction with Art. 5 para. 1, para. 2 GDPR. Overall, the measures to be taken are data security measures and measures to ensure a level of protection appropriate to the risk in terms of confidentiality, integrity, availability and resilience of the systems. In doing so, the state of the art, the implementation costs and the type, scope and purpose of the processing as well as the different probability of occurrence and severity of the risk for the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR shall be taken into account [details in Annex 1].
- (6) The technical and organisational measures are subject to technical progress and further development. In this respect, the Contractor is permitted to implement alternative adequate measures. The safety level of the defined measures must not be undercut. Material changes must be documented.

4. Rectification, limitation and erasure of data

- (3) The contractor may not correct, delete or restrict the processing of the data processed on behalf of the Customer without authorisation, but only in accordance with the documented instructions of the Customer. If a person concerned directly addresses the Contractor in this respect, the Contractor shall immediately forward this request to the Customer.
- (4) 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 duties of the contractor

In addition to compliance with the provisions of this contract, the Contractor shall have statutory obligations pursuant to Art. 28 to 33 GDPR; to this extent, the Contractor shall in particular ensure compliance with the following

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

requirements:

- i) Written appointment of a data protection officer who carries out his duties in accordance with Art. 38 and 39 GDPR. His contact details will be communicated to the Customer for the purpose of direct contact. The Customer will be informed immediately of any change in the data protection officer.
- j) Maintaining confidentiality pursuant to Art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 GDPR. In carrying out the work, the Contractor shall only employ employees who are obliged to maintain confidentiality and who have been familiarised beforehand with the relevant data protection provisions. The Contractor and any person under its authority who has access to personal data may process such data only in accordance with the instructions of the Customer, including the powers conferred by this Agreement, unless they are required to do so by law.
- k) The implementation of and compliance with all technical and organisational measures required for this contract pursuant to Art. 28 para. 3 sentence 2 lit. c, 32 GDPR [details in Annex 1].
- l) The contracting authority and the contractor shall, on request, cooperate with the Supervisory Authority in the performance of its tasks.
- m) Immediate information to the contracting authority on control actions and measures taken by the supervisory authority in so far as they relate to this contract. This shall also apply if a competent authority investigates the processing of personal data in the course of an administrative offence or criminal proceeding at the contractor's premises.
- n) Insofar as the Customer is subject to inspection by the supervisory authority, administrative offence or criminal proceedings, the liability claims of a person concerned or a third party or any other claim in connection with the processing of the order by the Contractor, the Contractor shall support the Customer to the best of its ability.
- o) The Contractor shall regularly monitor internal processes and technical and organisational measures in order to ensure that processing within its sphere of responsibility is carried out in accordance with the requirements of the applicable data protection legislation and that the rights of the data subject are protected.
- p) Verifiability of the technical and organisational measures taken vis-à-vis the Customer within the scope of his control powers in accordance with Section 7 of this contract.

6. Subcontracting relationships

- (4) For the purposes of this Regulation, subcontracting is defined as services which relate directly to the provision of the principal service. This does not include ancillary services which the contractor uses, e.g. as telecommunications services, postal/transport services, maintenance and user services 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. The Contractor shall, however, be obliged to take appropriate and legally compliant contractual agreements and control measures to guarantee the data protection and data security of the Customer's data even in the case of outsourced ancillary services.
- (5) Approved subcontractors are listed in Appendix 3 to the Cloud Contract.
- (6) The Contractor may not commission any subcontractors (further contract processors) without the consent of the Customer.

7. Control rights of the Customer

- (1) The Customer shall have the right to carry out inspections in consultation with the Contractor or to have them carried out by inspectors to be appointed 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 obligations of the Contractor under Art. 28 GDPR have been complied with. The Contractor undertakes to provide the Customer with the necessary information upon request and, in particular, to prove the implementation of the technical and organisational measures.
- (3) The proof of such measures, which do not only concern the concrete order, can be done by
 - compliance with approved rules of conduct pursuant to Art. 40 GDPR;

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

- certification in accordance with an approved certification procedure pursuant to Art. 42 GDPR;
- Current certificates, reports or report extracts from independent bodies (e.g. auditors, auditors, data protection officers, IT security department, data protection auditors, quality auditors);
- a suitable certification through an IT security or data protection audit (e.g. according to BSI-Grundschutz).

(4) The contractor may claim remuneration to enable the contracting authority to carry out checks.

8. notification in the event of violations by the contractor

- (3) The Contractor shall assist the Customer in complying with the obligations set out in Articles 32 to 36 of the GDPR regarding the security of personal data, reporting obligations in the event of data breakdowns, data protection impact assessments and prior consultations. This includes among others
- f) ensuring an adequate level of protection through technical and organisational measures which take into account the circumstances and purposes of the processing and the predicted likelihood and severity of a possible breach of rights due to security vulnerabilities and allow the immediate detection of relevant breach events
 - g) the obligation to report violations of personal data to the Customer without delay
 - h) the obligation to assist the contracting authority within the framework of its duty to inform the data subject and to make all relevant information available to the data subject without delay in this connection
 - i) the support of the Customer for his data protection impact assessment
 - j) the support of the Customer within the framework of prior consultations with the supervisory authority
- (4) For support services which are not included in the service description or are not due to a misconduct of the contractor, the contractor can claim a remuneration.

9. authority of the Customer to issue instructions

- (3) Oral instructions shall be confirmed by the Customer without delay (at least in text form).
- (4) The contractor must inform the Customer immediately if he is of the opinion that an instruction violates data protection regulations. The contractor is entitled to suspend the execution of the corresponding instruction until it has been confirmed or changed by the Customer.

10. deletion and return of personal data

- (4) Copies or duplicates of the data will not be made without the knowledge of the Customer. Excluded from this are backup copies, insofar as they are necessary to ensure proper data processing, as well as data which are necessary with regard to compliance with statutory storage obligations.
- (5) 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 as well as data stocks which have come into his possession and which are related to the contractual relationship, or, after prior consent, destroy them in accordance with data protection regulations. The same applies to test and scrap material. The deletion log shall be provided on request.
- (6) Documentation which serves as proof of the orderly and proper data processing shall be kept by the contractor in accordance with the respective retention periods beyond the end of the contract. He may hand them over to the Customer to discharge him at the end of the contract.

Annex - Technical and organisational measures implemented by CanDo

1. Confidentiality (Art. 32 para. 1 lit. b GDPR)

- Access control
No unauthorized access to data processing systems: keys, electric door openers, alarm systems
- Access control
No unauthorized system use: (Secure) passwords, automatic locking mechanisms, two-factor authentication, disk encryption;
- Access control
No unauthorized reading, copying, modification or removal within the system: authorization concepts and demand-oriented access rights, logging of accesses;
- Separation control
Separate processing of data collected for different purposes: Multi-Customer capability;

2. Integrity (Art. 32 para. 1 lit. b GDPR)

- Disclosure control
No unauthorized reading, copying, modification or removal during electronic transmission or transport: encryption, Virtual Private Networks (VPN), electronic signature;
- Input control
Determine whether and by whom personal data have been input, altered or removed into data processing systems: Logging, document management;

3. Availability and resilience (Art. 32 para. 1 lit. b GDPR)

- Availability control
Protection against accidental or deliberate destruction or loss: backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), virus protection, firewall, reporting paths and emergency plans;
- Rapid recoverability (Art. 32 para. 1 lit. c GDPR);

4. Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

- Data Protection Management;
- Incident-Response Management.

AWS Security Standards (Amazon)

Capitalised terms not otherwise defined in this document have the meanings assigned to them in the Agreement.

1. Information Security Program. AWS will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorised access to the AWS Network, and (c) minimise security risks, including through risk assessment and regular testing. AWS will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

1.1 Network Security. The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats.

1.2 Physical Security

1.2.1 Physical Access Controls. Physical components of the AWS Network are housed in nondescript facilities (the "Facilities"). Physical barrier controls are used to prevent unauthorised entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorised employees or contractors while visiting the Facilities.

1.2.2 Limited Employee and Contractor Access. AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access

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

privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its Affiliates.

1.2.3 Physical Security Protections. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorised access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All

AWS GDPR Data Processing Addendum 9

physical access to the Facilities by employees and contractors is logged and routinely audited.

2. Continued Evaluation. AWS will conduct periodic reviews of the security of its AWS Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. AWS will continually evaluate the security of its AWS Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.