Datenschutzvereinbarung zur Auftragsverarbeitung
gemäß Art. 28 Datenschutz-Grundverordnung (DS-GVO)

zwischen

Can Do GmbH

Implerstr. 26, 81371 München

- Auftragsverarbeiter -

und

KUNDE

- Verantwortlicher –

§ 1 Gegenstand und Dauer des Auftrags, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen

Gegenstand und Dauer des Auftrags, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen des Auftrags ergeben sich aus **Anlage 1**.

Die Verarbeitung der personenbezogenen Daten findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung der Datenverarbeitung, Datenübermittlung oder anderweitige Datenweitergabe in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen.

§ 2 Weisungsgebundene Verarbeitung und Remonstrationspflicht

Der Verantwortliche ist für die Einhaltung der anzuwendenden Datenschutzvorschriften im Hinblick auf die Zulässigkeit verantwortlich. Die Verarbeitung von Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarung und nach Weisung des Verantwortlichen. Der Verantwortliche behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Verarbeitung vor, dass er durch Einzelanweisungen konkretisieren kann. Weisungen des Verantwortlichen sind zu dokumentieren.

Sofern der Auftragsverarbeiter hiervon abweichend durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, zu einer Verarbeitung verpflichtet ist, teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, es sei denn, das betreffende Recht verbietet solche Mitteilung wegen eines wichtigen öffentlichen Interesses.

Weisungen werden vom Verantwortlichen grundsätzlich in Textform (z.B. per E-Mail) erteilt. Soweit eine Weisung ausnahmsweise mündlich erfolgt, wird diese vom Auftragsverarbeiter entsprechend in Textform (z.B. per E-Mail) bestätigt.

Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darauf hinweisen, wenn die Befolgung einer vom Verantwortlichen erteilten Weisung nach seiner Ansicht gegen die DS-GVO oder eine andere Vorschrift über den Datenschutz verstößt (Remonstrationspflicht).

§ 3 Vertraulichkeits-/ Verschwiegenheitspflicht

Der Auftragsverarbeiter wird zur Durchführung des Vertrages nur Personen beschäftigen, die er zur Vertraulichkeit verpflichtet hat oder die einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

§ 4 Sicherheit der Verarbeitung / Technische und organisatorische Maßnahmen gemäß Art. 32 DS-GVO

Der Auftragsverarbeiter ergreift alle erforderlichen technischen und organisatorischen Maßnahmen gem. Art. 32 DS-GVO. Diese werden in **Anlage 2** spezifiziert.

Sofern der Auftragsverarbeiter keine Zugriffsmöglichkeit auf die Daten des Verantwortlichen hat und die Auftragsverarbeitung vollumfänglich durch einen weiteren Auftragsverarbeiter (Subdienstleister) durchführt wird, ist in der **Anlage 2** das Sicherheitskonzept im Sinne des Art. 32 DS-GVO dieses weiteren Auftragsverarbeiters zu beschreiben.

Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Während der Dauer dieses Auftrags sind diese durch den Auftragsverarbeiter fortlaufend an die Anforderungen dieses Auftrags anzupassen und dem technischen Fortschritt entsprechend weiterzuentwickeln. Das Sicherheitsniveau der hier und in **Anlage 2** festgelegten technischen und organisatorischen Maßnahmen darf nicht unterschritten werden. Das Datensicherheitskonzept ist regelmäßig vorzulegen.

Der Auftragsverarbeiter verpflichtet sich, Änderungen der technischen und organisatorischen Maßnahmen, die einen wesentlichen Einfluss auf das gewährleistete Sicherheitsniveau haben, als Ergänzung der **Anlage 2** schriftlich zu dokumentieren, was auch in einem elektronischen Format erfolgen kann, und dem Verantwortlichen zur Kenntnis zu geben.

§ 5 Inanspruchnahme der Dienste weiterer Auftragsverarbeiter

Die zum Zeitpunkt des Vertragsschlusses in Anspruch genommenen weiteren Auftragsverarbeiter (Subdienstleister) sind in **Anlage 3** zu diesem Vertrag aufgeführt (soweit

einschlägig). Dem Auftragsverarbeiter wird eine Zustimmung zur Einbeziehung der in **Anlage 3** aufgeführten Auftragsverarbeiter erteilt.

Der Auftragsverarbeiter nimmt darüber hinaus keine weiteren Auftragsverarbeiter (Subdienstleister) ohne gesonderte schriftliche Zustimmung des Verantwortlichen, die auch in einem elektronischen Format erfolgen kann, in Anspruch.

Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters (Subdienstleister) in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem Subdienstleister im Wege eines Vertrags, der schriftlich abzufassen ist, was auch in einem elektronischen Format erfolgen kann, oder im Rahmen eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in diesem Vertrag festgelegt sind. Dabei müssen insbesondere hinreichende Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO erfolgt. Kommt der Subdienstleister seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes Subdienstleisters.

§ 6 Mitwirkungs-/ Unterstützungspflichten

Der Auftragsverarbeiter unterstützt den Verantwortlichen angesichts der Art der Verarbeitung mit geeigneten technischen organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DS-GVO genannten Rechte der betroffenen Person nachzukommen. Diese umfassen insbesondere die Berücksichtigung von Betroffenenrechten hinsichtlich der Gewährleistung von Transparenz, das Recht auf Auskunft, das Berichtigungsrecht, das Recht auf Löschung und „Vergessenwerden“, das Recht auf Einschränkung der Verarbeitung, das Mitteilungsrecht bei Berichtigung und Löschung sowie Einschränkung der Verarbeitung, das Recht auf Datenübertragbarkeit, das Widerspruchsrecht sowie die Rechte bei automatisierten Einzelfallentscheidungen.

§ 7 Unterstützung zur Pflichterfüllung des Verantwortlichen

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DS-GVO genannten Pflichten. Diese umfassen insbesondere die Gewährleistung der Sicherheit der Verarbeitung, die Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörden, die Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, die Datenschutz-Folgenabschätzung sowie die vorherige Konsultation einer der zuständigen Aufsichtsbehörde.

§ 8 Löschung und Rückgabe personenbezogener Daten

Soweit gesetzliche oder anderweitige Aufbewahrungspflichten nicht entgegenstehen, wird der Auftragsverarbeiter nach Beendigung des Auftrags die verwendeten personenbezogenen Daten dem Verantwortlichen in einer für den Verantwortlichen lesbaren und bearbeitbaren Form herausgeben, soweit der Verantwortliche ihn nicht anweist, die personenbezogenen Daten zu löschen. Sofern der Auftragsverarbeiter die Daten herausgibt, hat er etwaige Kopien in seinem Verantwortungsbereich unverzüglich zu löschen, nachdem der Verantwortliche den ordnungsgemäßen Eingang der Daten bestätigt hat.

Des Weiteren wird der Auftragsverarbeiter alle angemessenen Maßnahmen einleiten, um einen fortwährenden, unzulässigen Zugriff auf die Daten des Verantwortlichen auszuschließen.

Dokumente zum Nachweis der Einhaltung dieser Vereinbarung sind bei Vertragsende vom Auftragsverarbeiter einen angemessenen Zeitraum über das Vertragsende hinaus aufzubewahren und bei Bedarf herauszugeben.

§ 9 Pflichtennachweis und Unterstützung bei Überprüfungen

Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten zur Verfügung. Er ermöglicht Überprüfungen - einschließlich Inspektionen -, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und trägt zu ihrer Durchführung bei.

§ 10 Weitere Pflichten

Der Auftragsverarbeiter sichert zu, dass er, soweit gesetzlich erforderlich, einen Datenschutzbeauftragten benannt hat.

Bei Verdacht auf Datenschutzverletzungen oder anderen Störungen bei der Verarbeitung der personenbezogenen Daten des Verantwortlichen sowie bei Kontrollen und Maßnahmen der zuständigen Aufsichtsbehörde beim Auftragsverarbeiter ist der Verantwortliche unverzüglich zu informieren. Soweit ein Betroffener sich unmittelbar an den Auftragsverarbeiter zwecks Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DS-GVO genannten

Rechte der betroffenen Person wendet, wird der Auftragsverarbeiter diesen Antrag an den Verantwortlichen weitergeben und dessen Weisung hierzu abwarten.

Der Auftragsverarbeiter hat insbesondere mit der gebotenen Sorgfalt darauf hinzuwirken, dass seine Beschäftigten die gesetzlichen Bestimmungen zum Datenschutz beachten und die aus dem Bereich des Verantwortlichen erlangten Informationen nicht an Dritte weitergeben oder sonst verwerten. Auf Verlangen des Verantwortlichen ist vom Auftragsverarbeiter die erfolgte datenschutzrechtliche Schulung und Verpflichtung nachzuweisen.

§ 11 Sonstige Regelungen

Sollte die auftragsgemäße Erfüllung des Auftragsgegenstandes gem. § 1 dieser Vereinbarung beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder ein Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich. Der Auftragsverarbeiter wird alle in diesem Zusammenhang Beteiligte unverzüglich darüber informieren, dass die Verfügungsbefugnisse an den Daten ausschließlich beim Verantwortlichen liegen.

Bei etwaigen Widersprüchen zwischen diesem Vertrag und einem Hauptvertrag gehen die Regelungen dieses Vertrags den Regelungen des Hauptvertrags vor.

Sollten einzelne Teile dieses Auftrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

Jede Veränderung dieser Vereinbarung einschließlich ihrer Kündigung und dieser Klausel bedarf der Schriftform, was auch in einem elektronischen Format erfolgen kann.

* Unterschriften folgen *

[**München**], den [**Datum**]

[den [**Datum**].

_____	_____
- *Auftragsverarbeiter* - (Auftragnehmer)	(Auftraggeber)
_____	_____
- *Auftragsverarbeiter* -	

Anlagen

Anlage 1: „Allgemeine Angaben zum Vertrag“

Anlage 2: „Technische und organisatorische Maßnahmen“

Anlage 3: „Weitere Auftragsverarbeiter (Subdienstleister)“

Anlage 1

Allgemeine Angaben zum Vertrag

1. Gegenstand des Auftrags

Gegenstand des Auftrags ist: Bereitstellung des Cloud-Services Can Do-Ressourcenplanungssoftware

2. Dauer des Auftrags

☐Der Auftrag beginnt am … und endet am …

☒ Der Auftrag beginnt mit Unterzeichnung dieses Vertrags und wird auf unbestimmte Zeit geschlossen. Er ist mit einer Frist von 1 Monat kündbar. Die Möglichkeit zur fristlosen Kündigung aus besonderem Grund bleibt hiervon unberührt.

☐ Der Auftrag wird zur einmaligen Ausführung in folgendem Zeitraum geschlossen…

3. Art und Zweck der Datenverarbeitung

Die Tätigkeit des Auftragsverarbeiters dient

den folgenden Zwecken:

- **Bereitstellung und Betrieb der Onlineplattform**
- **Support und Wartung der Plattform und/oder des darauf betriebenen Dienstes**
- **Bereitstellung von Nutzungsreports**

4. Art der personenbezogenen Daten (Datenarten)

Folgende Datenarten sind Gegenstand dieses Auftrags:

Allgemeine Daten / Private Kontaktinformationen

☒Namen
☐ Private Adressdaten
☐ Nationalität
☐ Ausweisdaten / IDs
☐Geburtsdaten / Alter
☒ (Personen-)Profile

Vertragsdaten

☐ Vertragsdaten
☐ Abrechnungs- und Zahlungsdaten
☐ Bankverbindungsdaten / Kreditkartendaten
☐ Vertrags- / Nutzungshistorien

Dienste- und IT-(Nutzungs) Daten

☐ Gerätekennungen
☒ Zugangsdaten
☒ Identifikationsdaten / IDs
☒ Telekommunikationsdaten / Nachrichteninhalte
☒ Nutzungs- und Verbindungsdaten / Metadaten
☐ Bild-/Videodaten
☐ Audio-/Sprachdaten

Fahrzeug-, Standort- und Kontextdaten
☐Fahrzeugkennungen / -identifikationsdaten / FIN
☐Fahrzeug- / Fahrzeugzustands- / Fahrzeuganalysedaten
☐ Kontext- und Umgebungsinformationen
☐ Standort- / standortbezogene Daten / Bewegungsdaten

Berufliche Daten
☐ Stammdaten
☐ Lohn-/Gehaltsdaten / Einkommen
☐ Qualifikationen / Entwicklungspotentiale / Berufsprofile
☐ Gesundheits- / Sozialdaten
☐ Arbeitszeitdaten
☐ Sonderkonditionen
☐ Reisebuchung /-abrechnungsdaten
☐Workflows

Bonitätsdaten
☐Zahlungsverhalten
☐Scorewerte
☐Vermögensinformationen

Besondere Kategorien personenbezogener Daten
☐ Rassische / Ethnische Herkunft
☐ Politische Meinungen
☐ religiöse / weltanschauliche Überzeugungen
☐ Gewerkschaftszugehörigkeit
☐ Genetische Daten
☐ Biometrische Daten
☐ Gesundheitsdaten
☐ Daten zum Sexualleben / zur sexuellen Orientierung

☐ **Sonstige:**

5. Kategorien betroffener Personen

Im Wege der Auftragserfüllung verwendet der Auftragsverarbeiter personenbezogene Daten

Folgende Kategorien betroffener Personen sind Gegenstand des Auftrags:

☐ Kunden
☐ Interessenten
☐ Abonnenten
☐ Dienstnutzer
☐ Mittelbar Betroffene / Personen im Umfeld / Insassen
☐ Besucher
☐ Veranstaltungsteilnehmer
☐ Kommunikationsteilnehmer

☐ Bewerber
☒ Mitarbeiter
☐ ehemalige Mitarbeiter
☐ Auszubildende / Praktikanten
☐ Angehörige von Mitarbeitern

☐ Gesellschafter / Organe
☐ Geschäftspartner
☐ Lieferanten und Dienstleister
☐ Berater
☐ Dienstliche Ansprechpartner
☐ Handelsvertreter

☐ Pressevertreter

☐ Sonstige:

6. Regelmäßige Vorlage des Datensicherheitskonzepts

Eine aktuelle Fassung der in der **Anlage 2** aufgeführten technischen und organisatorischen Maßnahmen sowie ggf. das Datensicherheitskonzept und/oder Zertifikate bezüglich der Datensicherheit sind in regelmäßigen Abständen von 12 Monaten dem Verantwortlichen vorzulegen.

Anlage 2

Technische und organisatorische Maßnahmen

Unter Berücksichtigung des

- Stands der Technik,
- der Implementierungskosten und
- der Art, des Umfangs, der Umstände und
- der Zwecke der Verarbeitung sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

trifft der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch - ob unbeabsichtigt oder unrechtmäßig - Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Sofern der Auftragsverarbeiter keine Zugriffsmöglichkeit auf die Daten des Verantwortlichen hat und die Auftragsverarbeitung vollumfänglich durch einen oder mehrere weitere Auftragsverarbeiter (Subdienstleister) durchführt wird, sind in der Anlage 2 die Sicherheitskonzepte im Sinne des Art 32 DS-GVO dieser Subdienstleister zu beschreiben.

☒ **Der Auftragsverarbeiter ergreift folgende Maßnahmen:**

Bereitstellung einer AWS-Instanz im AWS-Rechenzentrum Frankfurt am Main.

☒ **Der Subdienstleister Amazon Web Services Inc. ergreift folgende Maßnahmen:**

Einrichtung und Betrieb der Cloud-Plattform gemäß GDPR Compliance on AWS-Dokument. Anhang zu diesem Dokument.

1. Pseudonymisierung

Personenbezogene Daten des Verantwortlichen können in einer Weise verarbeitet werden, sodass sie ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die eine unbefugte Identifizierung der Betroffenen ausschließen.

Gleichwohl bleiben derart pseudonymisierte Daten personenbezogene Daten im Sinne der DS-GVO. Die Pseudonymisierung ist eine technische und organisatorische Maßnahme, und kann vom Auftragsverarbeiter wie folgt umgesetzt werden:

☐ getrennte Speicherung von Zusatzinformationen zur Identifikation
☐Verwendung von (Personal-, Kunden- oder Patienten-) Kennziffern statt Namen
☐ Verschlüsselung von Zusatzinformationen zur Identifikation
☐Verwaltung und Dokumentation von differenzierten Berechtigungen auf die Zusatzinformationen zur Identifikation
☐Autorisierungsprozess oder Genehmigungsroutinen für Berechtigungen zur Verarbeitung von Zusatzinformationen zur Identifikation
☐ Kopierschutz hinsichtlich Zusatzinformationen zur Identifikation
☐ Vier-Augen-Prinzip für Identifikation
☐ Sonstiges/Spezifizierung der o.g. Maßnahmen: [**Bitte ausführen**]

2. Maßnahmen zur Verschlüsselung

☒ Verschlüsselung von mobilen Endgeräten wie Laptops, Tablets, Smartphones
☐Verschlüsselung von mobilen Speichermedien (CD/DVD- ROM, USB-Stick, externen Festplatten)
☐ Verschlüsselung von Dateien
☐ Verschlüsselung von Systemen/Anlagen
☒ Verschlüsselte Aufbewahrung von Passwörtern
☐ Verschlüsselung von Email bzw.- Email-Anhängen
☒ Gesicherte Datenweitergabe (z.B. SSL, FTPS, TLS)
☐ Gesichertes WLAN
☒ Sonstiges/Spezifizierung der o.g. Maßnahmen: Datentransfer über HTTPS

3. Maßnahmen zur Sicherstellung von Vertraulichkeit

a. Maßnahmen, durch die Unbefugten der Zutritt verwehrt wird:

☐ Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte)
☐ Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.)
☐ Sicherheitstüren / -fenster
☐ Gitter vor Fenstern/Türen
☐ Zaunanlagen
☐ Schlüsselverwaltung/Dokumentation der Schlüsselvergabe
☐ Werkschutz, Pförtner
☐ Alarmanlage
☐ Videoüberwachung
☐ Spezielle Schutzvorkehrungen des Serverraums
☐Spezielle Schutzvorkehrungen für die Aufbewahrung von Back-Ups und/oder sonstigen Datenträgern
☐ Nicht-reversible Vernichtung von Datenträgern
☐ Mitarbeiter- und Berechtigungsausweise
☐ Sperrbereiche

☐Besucherregelung (Bspw. Abholung am Empfang, Dokumentation von Besuchszeiten, Besucherausweis, Begleitung nach dem Besuch bis zum Ausgang)
☒ Sonstiges/Spezifizierung der o.g. Maßnahmen:

b. *Maßnahmen, die verhindern, dass Unbefugte die Verarbeitungssysteme nutzen können:*

☐Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
☐ Autorisierungsprozess für Zugangsberechtigungen
☐ Begrenzung der befugten Benutzer
☐ Single Sign-On
☐ Zwei-Faktor-Authentifizierung
☐ BIOS-Passwörter
☐Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)
☐Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unbefugtem Zugriff
☐ Personalisierte Chipkarten, Token, PIN-/TAN, etc.
☐ Protokollierung des Zugangs
☐ Zusätzlicher System-Log-In für bestimmte Anwendungen
☐Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)
☐ Firewall
☒ Sonstiges/Spezifizierung der o.g. Maßnahmen: Alles Sicherheitsmaßnahmen werden von Amazon Web Services Inc. durchgeführt

c. *Maßnahmen, die gewährleisten, dass nur berechtigte Personen auf die Verarbeitungssysteme zugreifen und personenbezogene Daten nicht unbefugt lesen, kopieren, verändern oder entfernen können:*

☒ Verwaltung und Dokumentation von differenzierten Berechtigungen
☐ Auswertungen/Protokollierungen von Datenverarbeitungen
☒ Autorisierungsprozess für Berechtigungen
☐ Genehmigungsroutinen
☒ Profile/Rollen
☐Verschlüsselung von CD/DVD- ROM, externen Festplatten und/oder Laptops (etwa per Betriebssystem, Safe Guard Easy, PGP)
☐Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf extern verwendbare Datenträger (z.B. Kopierschutz, Sperrung von USB-Ports, „Data Loss Prevention (DLP)-System“)
☐ „Mobile Device Management-System“
☐ Vier-Augen-Prinzip

☐ Funktionstrennung „Segregation of Duties“
☐ Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399
☒ Nicht-reversible Löschung von Datenträgern
☐ Sichtschutzfolien für mobile Datenverarbeitungssysteme
☐ Sonstiges/Spezifizierung der o.g. Maßnahmen:

d. *Maßnahmen die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:*

☒Speicherung der Datensätze in physikalisch getrennten Datenbanken
☒Getrennte Systeme
☒Zugriffsberechtigungen nach funktioneller Zuständigkeit
☒Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen
☒Mandantenfähigkeit von IT-Systemen
☐Verwendung von Testdaten
☒Trennung von Entwicklungs- und Produktionsumgebung
☐ Sonstiges/ Spezifizierung der o.g. Maßnahmen:

4. Maßnahmen zur Sicherstellung von Integrität

☒ Zugriffsrechte
☒ Systemseitige Protokollierungen
☐ Dokumenten Management System (DMS) mit Änderungshistorie
☐ Sicherheits-/Protokollierungssoftware
☒ Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten
☐ Mehraugenprinzip
☒Getunnelte Datenfernverbindungen (VPN = Virtuelles Privates Netzwerk)
☐ „Data Loss Prevention (DLP)-System“
☐ Elektronische Signatur
☐ Protokollierung von Datenübertragung oder Datentransport
☐ Protokollierung von lesenden Zugriffen
☒ Protokollierung des Kopierens, Veränderns oder Entfernens von Daten
☐ Sonstiges/Spezifizierung der o.g. Maßnahmen:

5. Maßnahmen zur Sicherstellung und Wiederherstellung von Verfügbarkeit

☒ Sicherheitskonzept für Software- und IT-Anwendungen
☒ Back-Up Verfahren
☒Aufbewahrungsprozess für Back-Ups (brandgeschützter Safe, getrennter Brandabschnitt, etc.)
☒ Gewährleistung der Datenspeicherung im gesicherten Netzwerk
☒ Bedarfsgerechtes Einspielen von Sicherheits-Updates
☒ Spiegeln von Festplatten

☒ Einrichtung einer unterbrechungsfreien Stromversorgung (USV)
☐ Geeignete Archivierungsräumlichkeiten für Papierdokumente
☒ Brand- und/oder Löschwasserschutz des Serverraums
☐ Brand- und/oder Löschwasserschutz der Archivierungsräumlichkeiten
☒ Klimatisierter Serverraum
☒ Virenschutz
☒ Firewall
☒ Notfallplan
☐ Erfolgreiche Notfallübungen
☐ Redundante, örtlich getrennte Datenaufbewahrung (Offsite Storage)
☐ Sonstiges/Spezifizierung der o.g. Maßnahmen:

6. Maßnahmen zur Sicherstellung der Belastbarkeit

☒ Notfallplan für Maschinenausfall
☒ Redundante Stromversorgung
☒ Ausreichende Kapazität von IT-Systeme und Anlagen
☒ Logistisch gesteuerter Prozess zur Verhinderung von Leistungsspitzen
☐ Redundanten Systeme/Anlagen
☐ Resilienz und Fehler-Management
☐ Sonstiges/Spezifizierung der o.g. Maßnahmen:

7. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

☒ Verfahren für regelmäßige Kontrollen/Audits
☐ Konzept für regelmäßige Überprüfung, Bewertung und Evaluierung
☐ Berichtswesen
☒ Penetrationstests
☐ Notfalltests
☒ Zertifizierung; falls vorhanden, AWS-Zertfikate (u.a. ISO9001 etc., siehe: https://aws.amazon.com/de/compliance/programs/)
☐ Sonstiges/Spezifizierung der o.g. Maßnahmen:

8. „Weisungskontrolle/Auftragskontrolle“

☒ Vertrag zur Auftragsdatenverarbeitung gem. Art. 28 Abs. 3 DS-GVO mit Regelungen zu den Rechten und Pflichten des Auftragsverarbeiters und Verantwortlichen
☐ Prozess zur Erteilung und/oder Befolgung von Weisungen
☒ Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
☒ Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
☐Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragsverarbeiter

☐ Unabhängige Auditierung der Weisungsgebundenheit
☒ Verpflichtung der Mitarbeiter zur Vertraulichkeit
☐ Vereinbarung von Konventionalstrafen für Verstöße gegen Weisungen
☒ Benennung eines Datenschutzbeauftragten gemäß Art. 37 ff. DS-GVO
☐ Datenschutzmanager/-koordinator
☒ Führen eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DS-GVO
☐ Dokumentations- und Eskalationsprozess für Verletzungen des Schutzes personenbezogener Daten
☐ Richtlinien/Vorgaben zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Sicherheit der Verarbeitung
☒ Prozess zur Weiterleitung von Betroffenenanfragen
☐ Sonstiges/Spezifizierung der o.g. Maßnahmen:

Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 DS-GVO oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 DS-GVO als Faktor zum Nachweis der Erfüllung der oben genannten Anforderungen (1. bis 8.):

☐

Anlage 3

Weitere Auftragsverarbeiter (Subdienstleister)

Name und Anschrift der Subdienstleister	Gegenstand der Unterbeauftragung	Datum des Vertrags zur Unterbeauftragung
AWS Deutschland, Marcel-Breuer-Strasse 12, 80807 München	Betrieb der AWS-Can Do-Cloud Plattform	1.3.2018