# Vertrag zur Auftragsverarbeitung

zwischen

Firmenname:

Straße + Hausnummer:

PLZ und Ort:

- als Verantwortlicher, im Folgenden bezeichnet als **„Auftraggeber“** -

Und der

**TNC System GmbH & Co. KG**

**Marburger Ring 32**

**35274 Kirchhain**

- als Auftragsverarbeiter, im Folgenden bezeichnet als **„Auftragnehmer“** -

**Präambel**

Der Auftraggeber möchte den Auftragnehmer mit den in § 3 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

**§ 1 Begriffsbestimmungen**

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DS-GVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gem. Art. 9 DS-GVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DS-GVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sowie genetische Daten gem. Art. 4 Abs. 13 DS-GVO, biometrischen Daten gem. Art. 4 Abs. 14 DS-GVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DS-GVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung ist gem. Art. 4 Abs. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie

das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(6) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DS-GVO eine von einem Mitgliedstaat gem. Art. 51 DS-GVO eingerichtete unabhängige staatliche Stelle.

**§ 2 Angabe der zuständigen Datenschutz-Aufsichtsbehörde**

(1) Zuständige Aufsichtsbehörde für beide Parteien ist Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, Gustav-Stresemann-Ring 1, 65189 Wiesbaden.

(2) Der Auftraggeber und der Auftragnehmer und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

**§ 3 Vertragsgegenstand**

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im IT-Umfeld. Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag (und der dazugehörigen Leistungsbeschreibung). Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben

**§ 4 Weisungsrecht**

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Die weisungsberechtigten Personen ergeben sich aus Anlage 5. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

**§ 5 Art der verarbeiteten Daten, Kreis der Betroffenen**

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in Anlage 1 näher spezifizierten personenbezogenen Daten.

(2) Der Kreis der von der Datenverarbeitung Betroffenen ist in Anlage 2 dargestellt.

**§ 6 Schutzmaßnahmen des Auftragnehmers**

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens die in Anlage 3 aufgeführten Maßnahmen der

a) Zutrittskontrolle
b) Zugangskontrolle
c) Zugriffskontrolle
d) Weitergabekontrolle
e) Eingabekontrolle
f) Auftragskontrolle
g) Verfügbarkeitskontrolle
h) Trennungskontrolle

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Beim Auftragnehmer ist als betrieblicher Datenschutzbeauftragter bestellt: gds – Gesellschaft für Datenschutz Mittelhessen mbH, Auf der Appeling 8, 35043 Marburg, Tel.: 06421 8041310, E-Mail: datenschutz@gdsm.de. Der Auftragnehmer veröffentlicht die Kontaktdaten des Datenschutzbeauftragten auf seiner Internetseite und teilt sie der Aufsichtsbehörde mit. Veröffentlichung und Mitteilung weist der Auftragnehmer auf Anforderung des Auftraggebers in geeigneter Weise nach.

(4) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

**§ 7 Informationspflichten des Auftragnehmers**

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DS-GVO liegen.

(5) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 6 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(6) Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten/Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich mitzuteilen.

(7) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DS-GVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

(8) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

**§ 8 Kontrollrechte des Auftraggebers**

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

(4) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 6 Abs. 4 auf Verlangen nach.

**§ 9 Einsatz von Subunternehmern**

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in Anlage 4 genannten Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt, soweit er den Auftraggeber hiervon vorab in Kenntnis setzt und dieser der Beauftragung des Subunternehmers zustimmt oder nicht innerhalb von 14 Tagen widerspricht. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der

Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

**§ 10 Anfragen und Rechte Betroffener,**

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DS-GVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

**§ 11 Haftung**

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

**§ 12 Außerordentliches Kündigungsrecht**

Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DS-GVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

**§ 13 Beendigung des Hauptvertrags**

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen. Zu entsorgende Unterlagen sind mit einem Aktenvernichter nach DIN 32757-1 zu vernichten. Zu entsorgende Datenträger sind nach DIN 66399 zu vernichten.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt

gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

**§ 14 Schlussbestimmungen**

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Kirchhain.

**Anlagen**

Anlage 1
Beschreibung der besonders schutzbedürftigen Daten/Datenkategorien

Anlage 2
Beschreibung der Betroffenen/Betroffenengruppen

Anlage 3
Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 4
Genehmigte Subunternehmer

Anlage 5
Weisungsberechtigte Personen

_____

**Datum, Unterschrift Auftraggeber**

_____

**Datum, Unterschrift Auftragnehmer**

**Anlage 1 - Beschreibung der Daten / Datenkategorien**

- ☐ Name, Vorname
- ☐ Geburtsdatum
- ☐ Anschrift/Adresse
- ☐ Telefonnummer
- ☐ E-Mail-Adresse
- ☐ Kommunikationsinhalte
- ☐ IP-Adresse
- ☐ Protokolldaten
- ☐ Benutzerkennungen
- ☐ Logdaten
- ☐ Metadaten
- ☐ Bankdaten
- ☐ Entgeltdaten
- ☐ weitere Identifikationsdaten (Personalausweisdaten etc.)
- ☐ Lokalisationsdaten (Aufenthaltsort, Wegstrecken etc.)
- ☐ Daten, welche die Verfolgung von Straftaten und Ordnungswidrigkeiten betreffen
- ☐ Daten, die dem Steuergeheimnis unterliegen
- ☐ Daten, die dem Sozialgeheimnis unterliegen
- ☐ Daten, die einem Berufsgeheimnis unterliegen
- ☐ Daten, die einem besonderen Amtsgeheimnis unterliegen
- ☐ Weitere personenbezogene Daten:

**Besondere Kategorien personenbezogener Daten (Art. 9 DS-GVO):**

- ☐ Rassische und ethnische Herkunft
- ☐ Politische Meinung
- ☐ Religiöse oder weltanschauliche Überzeugungen
- ☐ Gewerkschaftszugehörigkeit
- ☐ Genetische Daten
- ☐ Biometrische Daten
- ☐ Gesundheitsdaten
- ☐ Daten zum Sexualleben oder der sexuellen Orientierung

**Anlage 2 – Beschreibung der Betroffenen/Betroffenengruppen**

- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Kundinnen und/oder Kunden (Privatkunde)
- ☐ Ansprechpartner bei Kunden und Lieferanten (Geschäftskunden)
- ☐ Bürgerinnen und/oder Bürger
- ☐ Schülerinnen und/oder Schüler
- ☐ Studierende
- ☐ Patientinnen und/oder Patienten
- ☐ Sonstige:

**Anlage 3 – Technische und organisatorische Maßnahmen nach Art. 25, Art. 32 DS-GVO**

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

### Zutrittskontrolle

*Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.*

- ☒ Alarmanlage
- ☐ Automatisches Zugangskontrollsystem
- ☐ Schließsystem mit Codesperre
- ☐ Biometrische Zugangssperren
- ☒ Lichtschranken / Bewegungsmelder
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☐ Protokollierung der Besucher
- ☒ Sorgfältige Auswahl von Wachpersonal
- ☐ Absicherung von Gebäudeschächten
- ☒ Chipkarten-/Transponder-Schließsystem
- ☐ Manuelles Schließsystem
- ☐ Videoüberwachung der Zugänge
- ☐ Sicherheitsschlösser
- ☐ Personenkontrolle beim Pförtner / Empfang
- ☒ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Tragepflicht von Berechtigungsausweisen

### Zugangskontrolle

*Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.*

- ☒ Zuordnung von Benutzerrechten
- ☒ Passwortvergabe
- ☒ Authentifikation mit Benutzername / Passwort
- ☐ Gehäuseverriegelungen
- ☐ Sperren von externen Schnittstellen (USB etc.)
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☐ Protokollierung der Besucher
- ☒ Sorgfältige Auswahl von Wachpersonal
- ☒ Einsatz von Intrusion-Detection-Systemen
- ☐ Verschlüsselung von Smartphone-Inhalten
- ☒ Einsatz von Anti-Viren-Software
- ☒ Einsatz einer Hardware-Firewall
- ☒ Erstellen von Benutzerprofilen
- ☐ Authentifikation mit biometrischen Verfahren
- ☒ Zuordnung von Benutzerprofilen zu IT-Systemen
- ☒ Einsatz von VPN-Technologie
- ☐ Sicherheitsschlösser
- ☐ Personenkontrolle beim Pförtner / Empfang
- ☒ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Tragepflicht von Berechtigungsausweisen
- ☒ Verschlüsselung von mobilen Datenträgern
- ☒ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
- ☒ Verschlüsselung von Datenträgern in Laptops / Notebooks
- ☐ Einsatz einer Software-Firewall

### Zugriffskontrolle

*Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.*

- ☒ Erstellen eines Berechtigungskonzepts
- ☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert
- ☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☒ Physische Löschung von Datenträgern vor Wiederverwendung
- ☒ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- ☒ Verschlüsselung von Datenträgern
- ☒ Verwaltung der Rechte durch Systemadministrator
- ☒ Passwortrichtlinie inkl. Passwortlänge und -wechsel
- ☒ Sichere Aufbewahrung von Datenträgern
- ☒ Ordnungsgemäße Vernichtung von Daten-trägern (DIN 66399)
- ☒ Protokollierung der Vernichtung

### Trennungskontrolle

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

- ☐ Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☐ Erstellung eines Berechtigungskonzepts
- ☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern
- ☐ Festlegung von Datenbankrechten
- ☐ Logische Mandantentrennung (softwareseitig)
- ☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- ☐ Bei pseudonymisierten Daten: Trennung von Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- ☒ Trennung von Produktiv- und Testsystem

### Pseudonymisierung

- ☐
- ☐
- ☐
- ☐

*Es erfolgt keine Pseudonymisierung.*

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

### Weitergabekontrolle

*Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.*

- ☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☒ E-Mail-Verschlüsselung
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☒ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- ☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- ☒ Beim physischen Transport: Entsorgung mit sicheren Transportbehältern/-verpackungen

### Eingabekontrolle

*Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.*

- ☒ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- ☐ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

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

### Verfügbarkeitskontrolle

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

- ☒ Unterbrechungsfreie Stromversorgung (USV)
- ☒ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☒ Feuer- und Rauchmeldeanlagen
- ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☒ Testen von Datenwiederherstellung
- ☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☐ In Hochwassergebieten: Serverräume über der Wassergrenze
- ☒ Klimaanlage in Serverräumen
- ☒ Schutzsteckdosenleisten in Serverräumen
- ☒ Feuerlöschgeräte in Serverräumen
- ☒ Erstellen eines Backup & Recoverykonzepts
- ☒ Erstellen eines Notfallplans
- ☒ Serverräume nicht unter sanitären Anlagen

### Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

*Maßnahmen, die gewährleisten, dass nach einer Unterbrechung schnellstmöglich der Datenzugriff wiederhergestellt wird.*

- ☒ Vorhandenes Backup & Recoverykonzept
- ☐ Spiegelung der Daten auf dem Gelände
- ☐ Spiegelung der Daten an 2 Orten mit mehr als 10km Abstand

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

### Datenschutz-Management

*Maßnahmen, die gewährleisten, dass die Anforderung der DS-GVO nachprüfbar umgesetzt wurden.*

- ☒ Regelmäßige Datenschutz Audits
- ☐ DSMS vorhanden
- ☐ Interne Revision
- ☐ Externe Testierung / Prüfung
- ☐ Zertifizierungen:
- ☐ Sonstiges:

### Incident-Response-Management

*Maßnahmen, die gewährleisten, dass nach einer Störung der Auftraggeber eine Information über die Störung erhält, sofern dessen Daten betroffen waren.*

- ☒ Monitoring von Datenzugriffen
- ☒ Alarmsysteme bei Dateneinbruch
- ☒ Eskalations-Management vorhanden
- ☐ Testierung des Meldeprozesses
- ☐ Zertifizierung(en):
- ☐ Sonstiges:

### Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

*Maßnahmen, die gewährleisten, dass nach einer zeitlichen Vorgabe personenbezogene Daten gelöscht werden:*

- ☐ Manuelle Softwareunterstützung
- ☐ Automatische Softwareunterstützung
- ☐ Eigenentwicklungen
- ☒ Manuelle Löschung nach gesetzlicher Vorgabe
- ☒ Manuelle Löschung auf Anforderung
- ☐ Sonstiges:

## Auftragskontrolle

*Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.*

- ☒ Auswahl eines Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☒ Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag) i.S.d. Art. 28 DS-GVO
- ☒ Auftragnehmer hat Datenschutzbeauftragten bestellt
- ☐ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- ☐ Vertragsstrafen bei Verstößen
- ☐ Vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- ☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- ☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☐ Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

**Anlage 4 – Genehmigte Subunternehmer**

Die nachfolgenden Unternehmen sind genehmigte Subunternehmer im Sinne des § 9:

| **Firma Unterauftragnehmer** | **Anschrift** | **Leistung** |
|---|---|---|
| Teamviewer | TeamViewer Germany GmbH<br>Bahnhofsplatz 2<br>73033 Göppingen | Fernwartungssoftware |
| Docusnap | Docusnap GmbH<br>Franz-Larcher-Straße 4<br>83088 Kiefersfelden | Inventarisierungssoftware |
| Microsoft Corporation | Microsoft Deutschland GmbH<br>Walter-Gropius-Straße 5<br>80807 München | Supportdienstleistungen |

**Anlage 5 – Weisungsberechtigte Personen**

**Weisungsberechtigte Personen des Auftraggebers sind**

| | |
|---|---|
| **Name:** | |
| **Telefon:** | |
| **E-Mail:** | |

| | |
|---|---|
| **Name:** | |
| **Telefon:** | |
| **E-Mail:** | |

| | |
|---|---|
| **Name:** | |
| **Telefon:** | |
| **E-Mail:** | |

**Weisungsempfänger beim Auftragnehmer ist**

| | |
|---|---|
| Name: | Timo Nau |
| Telefon: | 06422/9282930 |
| E-Mail: | datenschutz@tnc-system.de |