

**Vertrag zur Auftragsdatenverarbeitung  
für die Instandhaltung und Pflege von AFZS-Fahrzeugausstattun-  
gen**

**zwischen**

---

als Verantwortlicher (hier bezeichnet als „Auftraggeber“)

**und**

---

als Auftragsverarbeiter (hier 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 gemäß 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 gemäß 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 gemäß 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 gemäß 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 gemäß Art. 10 DS-GVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen sowie genetische Daten gemäß Art. 4 Abs. 13 DS-GVO, biometrischen Daten gemäß Art. 4 Abs. 14 DS-GVO, Gesundheitsdaten gemäß Art. 4 Abs. 15 DS-GVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.
- (5) Verarbeitung ist gemäß 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 gemäß Art. 4 Abs. 21 DS-GVO eine von einem Mitgliedstaat gemäß Art. 51 DS-GVO eingerichtete unabhängige staatliche Stelle.

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

- (1) Zuständige Aufsichtsbehörde für den Auftraggeber ist der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg.
- (2) Zuständige Aufsichtsbehörde für den Auftragnehmer ist Landesbeauftragte für Datenschutz \_\_\_\_\_.
- (3) 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 die Auftraggeber Leistungen im Bereich der automatischen Fahrgastzählung auf Grundlage des mit Zuschlag geschlossenen Rahmenvertrags AFZS Instandhaltung / Pflege und der einzelnen Abrufe durch die EVB-IT Instandhaltungsverträge (Rahmenvertrag AFZS Instandhaltung / Pflege und EVB-IT Instandhaltungsverträge zusammen nachfolgend als „Hauptverträge“ bezeichnet). 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 den Hauptverträgen (und dem dazugehörigen Lastenheft). 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 der Hauptverträge vor.
- (3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit den Hauptverträgen in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die von dem Auftraggeber stammen oder für den Auftraggeber erhoben wurden.
- (4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit der Hauptverträge, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.
- (5) Die in diesem Vertrag vereinbarten Leistungen werden ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Leistungen oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

### **§ 4 Weisungsrecht**

- (1) Der Auftragnehmer darf Daten nur im Rahmen der Hauptverträge 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, zur weiteren Verarbeitung

verpflichtet, teilt er des Auftraggebers diese rechtlichen Anforderungen vor der Verarbeitung mit.

- (2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können von dem 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/die Nachfolger/-in bzw. Vertreter in Textform zu benennen.
- (3) Alle erteilten Weisungen sind sowohl von dem Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarten Leistungen hinausgehen, werden als Antrag auf Leistungsänderung behandelt.
- (4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er der Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung so lange 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 der Hauptverträge erhält der Auftragnehmer Zugriff auf die in Anlage 1 näher spezifizierten personenbezogenen Daten. Diese Daten umfassen keine besonderen Kategorien personenbezogener Daten; die einzusetzenden Kameras und Sensoren dürfen keine biometrischen Daten der betroffenen Personen erfassen, die eine eindeutige Identifizierung der Personen ermöglichen.
- (2) Der Kreis der von der Datenverarbeitung Betroffenen ist in Anlage 2 dargestellt.

## **§ 6 Pflichten und 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 Kenntnisaufnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

- (2) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen Daten für keine anderen Zwecke und insbesondere nicht für eigene Zwecke. Kopien der Daten werden, ohne dass sie im Auftrag oder in diesem Vertrag geregelt sind, nicht erstellt.
- (3) 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 gemäß 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
  - i) Pseudonymisierung
  - j) Wirksamkeitskontrolle

Er trifft diese technischen und organisatorischen Maßnahmen so, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt sind. Die in Anlage 3 beschriebenen technischen und organisatorischen Maßnahmen stellen das Datenschutzkonzept passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach dem Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO). Das Ergebnis samt vollständigem Auditbericht ist des Auftraggebers unaufgefordert vorzulegen.

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

- (4) Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit

die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicherzustellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen.

- (5) Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.
- (6) Im Falle einer Inanspruchnahme des Auftraggebers durch eine Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DS-GVO verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten zu unterstützen.
- (7) Beim Auftragnehmer ist ein betrieblicher Datenschutzbeauftragter/ein Ansprechpartner für den Datenschutz (sofern ein Datenschutzbeauftragter nach Art. 37 Abs. 1 DS-GVO nicht bestellt werden muss) bestellt. Dieser ergibt sich aus Anlage 5. 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.
- (8) 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 unaufgefordert 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 ihre 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 bei dem 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 gemäß Art. 30 Abs. 2 DS-GVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.
  - (8) An der Erstellung des Verfahrensverzeichnisses sowie bei erforderlichen Datenschutz-Folgeabschätzungen durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken und den Auftraggeber angemessen zu unterstützen. 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 und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann sie 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 sie den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt dem Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.
- (4) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.
- (5) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 6 Abs. 8 unaufgefordert 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 diese der Beauftragung des Subunternehmers vorab schriftlich zugestimmt hat.



Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit insbesondere unter Berücksichtigung der getroffenen technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO auszuwählen. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Verlangen zur Verfügung zu stellen. 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 ihre 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) Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat. Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen. Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden. Zudem sind die eingesetzten Mitarbeiter des Subunternehmers nach § 6 Abs. 8 zu verpflichten. Die Verpflichtungen sind dem Auftraggeber unaufgefordert in geeigneter Weise nachzuweisen.
- (3) 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. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

## **§ 10 Anfragen und Rechte Betroffener**

- (1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von ihren Pflichten nach Art. 12-22 sowie 32 und 36 DS-GVO.
- (2) Machen Betroffene Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich ihrer Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist die Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

## **§ 11 Haftung**

Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, haften die Parteien nach den gesetzlichen Vorschriften. Auf Art. 82 DS-GVO wird verwiesen.

## **§ 12 Außerordentliches Kündigungsrecht**

Der Auftraggeber kann die mit ihm abgeschlossenen Hauptverträge (EVB-IT Instandhaltungsverträge) 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. Eine etwaiges Kündigungsrecht des Rahmenvertragspartners VVS GmbH bezüglich der Rahmenverträge wegen solcher datenschutzrechtlichen Pflichtverletzungen des Auftragnehmers bleibt hiervon unberührt.

## **§ 13 Beendigung des Hauptverträge**

- (1) Der Auftragnehmer wird nach Beendigung der Hauptverträge oder jederzeit auf Anforderung des Auftraggebers 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 66399 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 der Hauptverträge hinaus die ihm im Zusammenhang mit den Hauptverträgen bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende der Hauptverträge hinaus so lange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm von dem Auftraggeber zugeleitet wurden oder die er für diese 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 Stuttgart.

\_\_\_\_\_, den \_\_\_\_\_

\_\_\_\_\_, den \_\_\_\_\_

\_\_\_\_\_  
Auftraggeber

\_\_\_\_\_  
Auftragnehmer

## **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; betrieblicher Datenschutzbeauftragter/ Ansprechpartner für den Datenschutz des Auftragnehmers

#### **Anlage 1 - Beschreibung der besonders schutzbedürftigen Daten/Datenkategorien:**

- Name
- Kontaktdaten
- Vertragsdaten
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsverkehrsdaten
- Position/Funktion
- GPS-Daten
- IP-Adressen
- Biometrische Daten

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

- Kunden
- Potenzielle Kunden/interessierte Kreise
- Mitarbeiter
- Auftragsverarbeiter
- Ansprechpartner

### Anlage 3 – Technische und organisatorische Maßnahmen des Auftragnehmers

Dokumentation der nach Art. 32 DS-GVO zu treffenden technischen und organisatorischen Maßnahmen

<p>1.</p>	<p><b>Zutrittskontrolle</b></p> <p>Maßnahmen, die es Unbefugten verwehren, sich den IT-Systemen, Datenverarbeitungsanlagen sowie vertraulichen Akten und Datenträgern physisch zu nähern</p>	<p>1.1 Bauliche Absicherung (Gebäudesicherheitskonzept, Protokollierung Zu- und Abgänge, Zutrittskontrollsystem, Überwachungseinrichtung)</p> <ul style="list-style-type: none"> <li>- Schutz der Gebäude oder Geschäftsräume durch angemessene Zutrittskontrollsysteme</li> <li>- Abhängig von der Sicherheitseinstufung werden Grundstücke, Gebäude oder einzelne Bereiche durch zusätzliche Maßnahmen gesichert.</li> <li>- Entsprechend des Schutzbedarfs sind Zutrittsberechtigungen zu den Sicherheitsräumen nochmals auf das Personal der zuständigen Fachabteilung eingeschränkt.</li> </ul> <p>1.2 Organisatorische Absicherung (Schlüsselordnung, -vergabe, Besucherausweise, Ausweisordnung)</p> <ul style="list-style-type: none"> <li>- Einsatz einer Schließanlage und Schlüssel mit Personen- und Zugangsidentifikation</li> <li>- Der Eingangsbereich ist durch einen Empfangsbereich überwacht, bei dem sich Gäste anmelden müssen.</li> <li>- Gäste werden durch die zu besuchende Person überwacht.</li> </ul> <p>1.3 Rechnerräume (Aufstellungsort Server)</p> <ul style="list-style-type: none"> <li>- Die Server sind in geeigneten Räumen untergebracht, Schutz gegen Feuer-, Wasser- und ähnliche Schäden wurde berücksichtigt, strikte Zugangsregeln.</li> </ul>
<p>2.</p>	<p><b>Benutzerkontrolle / Zugangskontrolle</b></p> <p>Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können</p>	<p>2.1 Kontrollmaßnahmen (Regelwerk, Benutzerregistrierung)</p> <ul style="list-style-type: none"> <li>- Das Benutzerkonto muss zunächst beantragt und vom Vorgesetzten genehmigt werden.</li> </ul> <p>2.2 Netzwerk (Freigabe von Netzzugängen)</p> <ul style="list-style-type: none"> <li>- Der Zugang über das LAN ist intern über anwendungsspezifische Kennwörter geschützt.</li> </ul>

		<ul style="list-style-type: none"> <li>- Der Zugang über das LAN von extern wird über eine Firewall geschützt.</li> </ul> <p>2.3 Wartung (Verbindungsaufbau Fernwartung, Mitnahmen DV-Equipment zu Wartungszwecken)</p> <ul style="list-style-type: none"> <li>- Es gibt vertragliche Regelungen zur Wartung/Fernwartung.</li> </ul> <p>2.4 Sonstiges (Kennwortverfahren, automatische Sperrung, Einrichtung eines Benutzerstammsatzes pro User, Verschlüsselung von (mobilen) Datenträgern und (mobiler) Systeme)</p> <ul style="list-style-type: none"> <li>- Die technischen Systeme und Anwendungen der Auftragnehmer sind durch eine Benutzer-/Kennwort-Abfrage geschützt.</li> <li>- Arbeitsplätze werden bei Verlassen von den Benutzern gegen unberechtigte Nutzung gesichert (Abmeldung) und nach einem angemessenen Zeitintervall automatisch gesichert (automatische Abmeldung).</li> <li>- Fremde haben keinen Zugriff auf die Systeme des Auftragnehmers</li> </ul>
3.	<b>Zugriffskontrolle</b>  Maßnahmen, damit die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können	<p>3.1 Zugriffsschutzmaßnahmen (Clean Desk, Sicherheitssoftware, Verschlüsselung, differenzierte Berechtigungen, Auswertungen, Kenntnisnahme, Veränderung, Löschung)</p> <ul style="list-style-type: none"> <li>- Die Systemzugänge der mit der Ausführung beauftragten Personen sind nur mit den Rechten ausgestattet, die für die Aufgabenerfüllung erforderlich sind.</li> <li>- Zur technischen Zugriffssicherung verwendet der Auftragnehmer anerkannte Sicherheitssysteme. Zugriffe werden technisch überwacht.</li> <li>- Eine Zugriffsberechtigung wird auf Basis des Berechtigungskonzepts beantragt und vom Vorgesetzten bzw. der Geschäftsleitung genehmigt.</li> <li>- Die Ausführung administrativer Zugriffe wird mit den Mitteln des Betriebssystems protokolliert. Auf die Anwendung bezogene Zugriffe werden mit den Mitteln und Möglichkeiten der Anwendung oder des Betriebssystems protokolliert und überwacht.</li> </ul>

		<p>3.2 Sichere Entsorgung (Sichere Entsorgung von Papierdokumenten und digitalen Informationen, Beachtung von Aufbewahrungsfristen)</p> <ul style="list-style-type: none"> <li>- Datenschutzrelevante Papierdokumente werden über einen Shredder nach DIN 66399 vernichtet.</li> <li>- Hardware, die Daten enthält, wird datenschutzgerecht vernichtet.</li> </ul>
4.	<p><b>Datenverarbeitungskontrolle / Weitergabekontrolle</b></p> <p>Maßnahmen, die bei der Übermittlung oder beim Transport von personenbezogenen Daten eingesetzt werden, um unberechtigte Zugriffe, insbesondere zum Lesen, Kopieren, Verändern oder Entfernen dieser Daten vermeiden</p>	<p>4.1 Physische Datenübergabe (Weitergabe von Datenträgern, Belege, Datenübergabe, Richtigkeit Adressat, Datenklassifizierung)</p> <ul style="list-style-type: none"> <li>- Fremde Datenträger dürfen nicht genutzt werden.</li> <li>- Datenträger zur internen Datenweitergabe werden verschlüsselt.</li> </ul> <p>4.2 Elektronische Datenübermittlung (Protokollierung, Transportsicherung wie Verschlüsselung / Tunnelverbindung (VPN), elektronische Signatur, Datenverschlüsselung)</p> <ul style="list-style-type: none"> <li>- Firewallsysteme und ständig aktualisierte Virenschutzsoftware sichern neben einer Verschlüsselung und dem Einsatz von VPN Technologie die Kommunikation zum Internet.</li> <li>- Alle Datentransfers mit Dritten werden verschlüsselt oder im Ausnahmefall mit Passwortschutz durchgeführt.</li> <li>- Der Versand von personenbezogenen Daten erfolgt immer verschlüsselt.</li> </ul>
5.	<p><b>Verantwortlichkeitskontrolle / Eingabekontrolle</b></p> <p>Maßnahmen, damit es möglich ist, festzustellen, wer welche personenbezogenen Daten zu welcher Zeit verarbeitet hat und wohin sie übermittelt werden sollen oder übermittelt worden sind</p>	<p>Protokolle (Protokollierung(ssysteme), Auswertungsarten, Aufbewahrung)</p> <ul style="list-style-type: none"> <li>- Auf die Anwendung bezogene Dateneingaben werden mit den Mitteln und Möglichkeiten der Anwendung oder des Betriebssystems protokolliert und überwacht.</li> </ul>
6.	<p><b>Auftragskontrolle</b></p> <p>Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im</p>	<p>6.1 Vorherige dokumentierte Prüfung, vertragliche Verpflichtung und Genehmigung von Unterauftragnehmern durch den Auftraggeber</p>

	<p>Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden</p>	<p>Weisungsgemäße Auftragsdatenverarbeitung (Kontrolle Einhaltung Weisung, Vereinbarung Subunternehmer, Identitätsprüfung)</p> <ul style="list-style-type: none"> <li>- Der Auftragnehmer wird sorgfältig ausgewählt.</li> <li>- Der Auftragnehmer bearbeitet die ihm überlassenen Daten nur aufgrund und anhand von vertraglich vereinbarten Weisungen des Auftraggebers.</li> <li>- Kompetenzen und Kontrollmaßnahmen werden in Abstimmung mit dem Auftraggeber definiert und technisch oder organisatorisch in die Betriebsabläufe eingebunden.</li> <li>- Sollten Dritte hinzugezogen werden, werden diese über entsprechende Auftragsdatenverarbeitungsvereinbarungen zur Einhaltung der Datenschutzmaßnahmen verpflichtet.</li> <li>- Die Mitarbeiter des Auftragnehmers müssen auf den Datenschutz verpflichtet werden.</li> <li>- Die Zugriffsberechtigten werden geschult und regelmäßig nachgeschult.</li> <li>- Alle Mitarbeiter und Dienstleister des Auftragnehmers mit Zugriff auf personenbezogene Daten werden verpflichtet, diese nur auf Anweisung und ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen zu verarbeiten.</li> </ul> <p>6.2 Meldung Datenschutzverstöße (Meldesystem, Schulung)</p> <ul style="list-style-type: none"> <li>- Die fristgerechte Meldung von Datenschutzverstößen wird durch interne Regelungen (Datenschutzrichtlinie, Schulungen) sichergestellt.</li> </ul>
7.	<p><b>Verfügbarkeitskontrolle</b></p> <p>Maßnahmen, die sicherstellen, dass personenbezogene Daten nicht unbeabsichtigt zerstört werden oder verloren gehen</p> <p>Es soll sichergestellt werden, dass personenbezogene Daten und der Zugang zu diesen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können</p>	<p>7.1 Risiko und Schwachstellenanalyse (Existenz, Prozess Beseitigung von Schwachstellen, aktives Patchmanagement, Notfallplan)</p> <ul style="list-style-type: none"> <li>- Regelmäßige Risikoanalysen werden durchgeführt</li> <li>- Die Aktualität der Systeme wird von zentraler Stelle sichergestellt.</li> <li>- Es existieren Pläne für Notfälle</li> </ul> <p>7.2 USV, Überspannungsschutz (Sicherheitsmaßnahmen, Dokumentation, Überwachung)</p>



		<ul style="list-style-type: none"> <li>- Die Serverräume sind mit USV ausgestattet</li> </ul> <p>7.3 Branderkennung (Frühwarnsystem, Rufanlage, Aufbewahrung, Schlüssel im Alarmfall)</p> <ul style="list-style-type: none"> <li>- Die Serverräume sind mit Meldesystemen für Brand und Rauchentwicklung ausgerüstet.</li> </ul> <p>7.4 Backupkonzept (Verantwortlichkeiten, Schutz vor Diebstahl, Funktionalitätstest)</p> <ul style="list-style-type: none"> <li>- Es existiert ein Backupkonzept / Back-Up von Daten auf Server</li> <li>- Diebstahlschutz</li> </ul> <p>7.5 Redundanz (Spiegeln von Informationen, z. B. RAID-Verfahren)</p> <ul style="list-style-type: none"> <li>- Daten werden vor versehentlichem sowie vorsätzlichem Ändern geschützt.</li> </ul> <p>7.6 Sonstiges (Getrennte Aufbewahrung, Virenschutz / Firewall)</p> <ul style="list-style-type: none"> <li>- Alle Server sind durch eine Firewall geschützt und es sind aktuelle Virens Scanner installiert.</li> </ul> <ul style="list-style-type: none"> <li>- Berechtigung zum Löschen (4-Augen-Prinzip)</li> </ul>
8.	<b>Trennungskontrolle</b> Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden können	<p>8.1 Mandantenfähigkeit (Durchgängigkeit, Dokumentation, Zweckbindung, klare Trennung)</p> <ul style="list-style-type: none"> <li>- Die Daten verschiedener Mandanten werden getrennt.</li> </ul> <p>8.2 Trennung von Entwicklungs-, Test-, Produktivsystem (Netztrennung, Anonymisierung, Systemtrennung)</p> <ul style="list-style-type: none"> <li>- Test- und Produktivsysteme werden getrennt.</li> <li>- Testsysteme arbeiten mit Dummy-Daten.</li> </ul>
9.	<b>Pseudonymisierung</b>	Pseudonymisierung (Ersetzen von Klardaten durch Pseudonyme)

	<p>Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern möglich und sinnvoll.</p>	<ul style="list-style-type: none"> <li>- Von den Möglichkeiten der Anonymisierung und der Pseudonymisierung wird wo immer möglich/erforderlich Gebrauch gemacht.</li> <li>- Insbesondere hinreichende Unkenntlichmachung bzw. „Verpixelung“ von Bild- und Videoaufnahmen und von durch elektronische Sensoren erzeugten Bildern und Darstellungen von Personen bei der Erstellung der Aufnahmen bzw. Erfassung der Personen durch die Kameras oder Sensoren (Datenerhebung)</li> </ul>
10.	<p><b>Wirksamkeitskontrolle</b></p> <p>Maßnahmen, die gewährleisten, dass die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sicherzustellen, regelmäßig überprüft, bewertet und evaluiert wird</p>	<p>Regelmäßige interne Prüfungen (Dokumentation, Penetrationstests)</p> <p>Regelmäßige externe Prüfungen (Bspw. Zertifikate, Penetrationstests)</p> <ul style="list-style-type: none"> <li>- Notfallübungen</li> </ul>

#### **Anlage 4 – Genehmigte Subunternehmer**

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

Unterauftragnehmer	Anschrift und Kontaktdaten	Leistung des Unterauftragnehmers

#### **Anlage 5 – Weisungsberechtigte Personen; betrieblicher Datenschutzbeauftragter der AG; betrieblicher Datenschutzbeauftragter/ Ansprechpartner für den Datenschutz des AN**

Weisungsberechtigte Personen des Auftraggebers sind:

---

Behördlicher Datenschutzbeauftragter des Auftraggebers:

---

Weisungsempfänger beim Auftragnehmer sind:

---

betrieblicher Datenschutzbeauftragter/Ansprechpartner für den Datenschutz des AN ist:

---