

Auftragsverarbeitungsvertrag (AVV) VAIR gemäß Art. 28 DSGVO (Datenschutz-Grundverordnung)

Mit dem Bestätigen des Absende-Buttons auf www.vaps.de/VAIR schließt der Auftraggeber die nachfolgende, von der VAPS GmbH verbindlich zur Annahme angebotene Vereinbarung zur Auftragsverarbeitung personenbezogener Daten mit der

VAPS GmbH, Kollberg 9, 30916 Isernhagen

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

§1 Vertragsgegenstand, Zweck, Kategorien der Daten und Betroffene

Gegenstand dieses Vertrages ist die Verarbeitung personenbezogener Daten (nachstehend „Daten“ genannt) durch den Auftragnehmer für den Auftraggeber in dessen Auftrag und nach dessen Weisung.

Zweck der Verarbeitung ist die Zurverfügungstellung von GW Vermarktungsdaten für die Analyse des Gebrauchtfahrzeugmarktes.

Folgende Kategorien von Daten werden verarbeitet: Kundenart, Postleitzahl, Fahrzeugdaten einschl. FIN / Ausstattungs- und Verkaufsdaten. Betroffene sind Privat- und Geschäftskunden des Auftraggebers.

§2 Verantwortlichkeiten

Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der Betroffenen nach den Art. 12 bis 22 DSGVO allein verantwortlich.

Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

Der Auftraggeber informiert den Auftragnehmer unverzüglich und vollständig, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

Es gelten die gesetzlichen Bestimmungen des Art. 82 DSGVO. Bei Widersprüchen zwischen anderen Vereinbarungen und diesem AVV geht die Regelung dieses AVV vor.

§3 Weisungsbefugnis des Auftraggebers

Die Weisungen sind vom Auftraggeber in schriftlicher Form oder in Textform zu erteilen, sofern Sie über die Regelungen dieses AVV hinausgehen. Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragnehmer eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird.

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§4 Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich personenbezogene Daten auf dokumentierte Weisung des Auftraggebers zu verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen der zuständigen Aufsichtsbehörde.

Hierzu gehören

- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;
- die Verpflichtung, Verstöße des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen oder weiterer vom Auftragnehmer beauftragter Auftragsverarbeiter gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen, unverzüglich an den Auftraggeber zu melden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten gegenüber der jeweils zuständigen Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen nach Artt. 33, 34 DSGVO;
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung, mit allen ihm zur Verfügung stehenden Informationen;
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen der Aufsichtsbehörde.

Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten Befugten zur Vertraulichkeit und falls erforderlich auf das Fernmeldegeheimnis verpflichtet haben. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Hauptvertrages fort.

Der Auftragnehmer verpflichtet sich, den Auftraggeber angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person zu unterstützen, ihm in diesem Zusammenhang relevante Informationen zur Verfügung zu stellen und Anfragen von Betroffenen an den Auftraggeber weiterzuleiten.

Der Auftragnehmer stellt auf Anfrage des Auftraggebers dem Auftraggeber alle Angaben zur Verfügung, die zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten im Sinne des Art. 30 Abs. 1 DSGVO benötigt werden.

Eine Verarbeitung außerhalb der Räumlichkeiten des Auftragnehmers (z.B. im Homeoffice) ist gestattet, sofern das vereinbarte Sicherheitsniveau nicht unterschritten wird.

Sollten die personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten beim Auftraggeber als Verantwortlichem im Sinne der DSGVO liegen.

§5 Technische und organisatorische Maßnahmen

Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen (**Anlage 2**) vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind dem Auftraggeber rechtzeitig vorab mitzuteilen.

§6 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Die Angaben zum Datenschutzbeauftragten und den Empfangsberechtigten sind in **Anlage 1** festgelegt.

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

- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen.
- Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

§7 Unterauftragsverhältnisse

Ein Einsatz von Unterauftragnehmern ist dem Auftragnehmer unter Einhaltung der folgenden Regelungen gestattet:

Der Auftragnehmer muss Unterauftragnehmer unter besonderer Berücksichtigung der Eignung hinsichtlich der Erfüllung der zwischen Auftraggeber und Auftragnehmer vereinbarten technischen und organisatorischen Maßnahmen gewissenhaft auswählen. Den Unterauftragnehmern ist im Wege eines Vertrags im Wesentlichen dieselben Pflichten aufzuerlegen, die in dieser Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind, insbesondere hinsichtlich der Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages sowie den beschriebenen Kontroll- und Überprüfungsrechten des Auftraggebers. Hierbei müssen ferner hinreichend Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Die Verarbeitung von Daten des Auftraggebers außerhalb der EU/EWR darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DSGVO erfüllt sind.

Nicht als Unterauftragsverhältnis im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung in Anspruch nimmt. Dazu zählen z. B. Telekommunikationsdienstleistungen, Reinigungskräfte und Maßnahmen zur Wartung sowie zur Sicherstellung der Vertraulichkeit, Integrität & Verfügbarkeit.

Der Auftragnehmer ist verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Für die zum Zeitpunkt der Vertragsunterzeichnung in der **Anlage 3** aufgeführten Dienstleister gilt die Zustimmung für das Tätigwerden als erteilt.

Der Auftragnehmer ist berechtigt weitere Unterauftragnehmer unter den vorher genannten Bedingungen einzusetzen und informiert den Auftraggeber rechtzeitig über die Hinzuziehung oder die Ersetzung von Unterauftragnehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

§8 Kontrollrechte des Auftraggebers

Der Auftraggeber hat den Auftragnehmer unter dem Aspekt ausgewählt, dass dieser hinreichenden Garantien dafür bietet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer regelmäßig Überprüfungen durchzuführen oder im Einzelfall durch zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen, sofern die untenstehenden Nachweise in begründeten Einzelfällen nicht ausreichend sein sollten.

Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO oder die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO oder aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren)
- eine geeignete Zertifizierung des eingesetzten Informations-Sicherheits-Management-Systems (z.B. TISAX, ISO 27001).

Für die Ermöglichung und Durchführung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen angemessenen Vergütungsanspruch geltend machen.

§9 Berichtigung, Einschränkung und Löschung von Daten

Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

Nach Abschluss der vertraglichen Arbeiten – oder früher nach Aufforderung durch den Auftraggeber – hat der Auftragnehmer alle im Rahmen des Auftrags in seinen Besitz gelangte Unterlagen oder Datenträger sowie personenbezogene Daten dem Auftraggeber auszuhändigen oder auf Anweisung des Auftraggebers datenschutzkonform zu löschen bzw. zu vernichten, sofern keine gesetzliche Pflicht zur Aufbewahrung besteht.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen, jedoch mindestens 3 Jahre, über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Sofern zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten entstehen, bedarf es einer vorherigen Vereinbarung (mindestens Textform) über die Kostentragung.

§10 Leistungsort

Der Auftraggeber stimmt einer Verlagerung eines Ortes der Leistungserbringung innerhalb des Leistungslandes und Länder, die Mitglied der EU/EWR sind, zu, wenn dort nachweislich ein gleiches Sicherheitsniveau gegeben ist und keine für den Auftraggeber geltenden gesetzlichen Bestimmungen gegen diese Verlagerung sprechen. Die Nachweispflicht hierzu liegt bei dem Auftragnehmer.

Wenn der Auftragnehmer die geschuldeten Leistungen ganz oder teilweise von einem Standort außerhalb der EU/EWR in einem sog. sicheren „Drittstaat“ erbringen möchte bzw. die Leistungserbringung dorthin zu verlagern plant, informiert der Auftragnehmer rechtzeitig den Auftraggeber.



Sofern der Auftraggeber nicht innerhalb einer Frist von zwei Wochen nach Zugang der Mitteilung gemäß Abs. 2 der Verlagerung unter Angabe von berechtigten Gründen nicht aktiv widerspricht, gilt die Zustimmung zu dieser Verlagerung seitens des Auftraggebers als erteilt.

Sofern die Datenverarbeitung nach dieser Vereinbarung und den gesetzlichen Vorgaben zur Verarbeitung personenbezogener Daten im Auftrag bzw. zur Übermittlung personenbezogener Daten in das Ausland zulässig außerhalb Deutschlands erbracht werden darf, wird der Auftragnehmer für die Einhaltung und Umsetzung der gesetzlichen Erfordernisse zur Sicherstellung eines adäquaten Datenschutzniveaus bei Standortverlagerungen und bei grenzüberschreitendem Datenverkehr Sorge tragen.

§11 Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträgern wird ausgeschlossen.

§12 Sonstiges

Die Laufzeit dieses AVV ist unbefristet. Er kann jederzeit von beiden Seiten mit einer Kündigungsfrist von 6 Monaten zum Monatsende in Textform gekündigt werden.

Nebenabreden bestehen nicht. Solche müssen grundsätzlich in Schriftform separat vereinbart werden.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Mit dem Bestätigen des Absende-Buttons auf www.vaps.de/VAIR ist der AVV wirksam und für beide Seiten verbindlich geschlossen.

Anlage 1 Empfangsberechtigte und Datenschutzbeauftragter

Zum Empfang von Weisungen betreffend die Auftragsdatenverarbeitung sind aufseiten des Auftragnehmers ausschließlich folgende Personen berechtigt:

Name	Position	Telefon	E-Mail
Dennis Skora	Leiter Vertrieb	05136 898 8008	datenschutz@vaps.de
Andreas Meier	Leiter Applikationen & Services	05136 898 6281	datenschutz@vaps.de
Alexander Salfeld	Informationssicherheitsbeauftragter	05136 898 6234	datenschutz@vaps.de

Beim Auftragnehmer ist folgende Person als Datenschutzbeauftragter bestellt:

Thomas Althammer, externer Datenschutzbeauftragter, 05113 306 0390, datenschutz@vaps.de, kontakt-dsb@althammer-kill.de

Anlage 2 Technische und organisatorische Maßnahmen**1 Zutrittskontrolle**

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

- | | |
|---|---|
| <input checked="" type="checkbox"/> Alarmanlage | <input checked="" type="checkbox"/> Chipkarten-/Transponder-Schließsystem |
| <input checked="" type="checkbox"/> Automatisches Zutrittskontrollsystem | <input checked="" type="checkbox"/> Manuelles Schließsystem |
| <input checked="" type="checkbox"/> Schließsystem mit Codesperre | <input checked="" type="checkbox"/> Videoüberwachung der Zugänge |
| <input checked="" type="checkbox"/> Protokollierung der Besucher | <input checked="" type="checkbox"/> Sicherheitsschlösser |
| <input checked="" type="checkbox"/> Sorgfältige Auswahl von Reinigungskräften | <input checked="" type="checkbox"/> Personenkontrolle beim Empfang |
| <input checked="" type="checkbox"/> Tragepflicht von Besucherausweisen | <input checked="" type="checkbox"/> Sorgfältige Auswahl von Reinigungskräften |

2 Zugangskontrolle

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

- | | |
|--|---|
| <input checked="" type="checkbox"/> Zuordnung von Benutzerrechten | <input checked="" type="checkbox"/> Einsatz von individuellen Benutzernamen |
| <input checked="" type="checkbox"/> Vorgaben für sichere Passwörter | <input checked="" type="checkbox"/> Einsatz von VPN-Technologie (Fernzugriff) |
| <input checked="" type="checkbox"/> Authentifikation Benutzername / Passwort | <input checked="" type="checkbox"/> Einsatz von Intrusion-Detection-Systemen |

3 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.

- | | |
|--|---|
| <input checked="" type="checkbox"/> Berechtigungskonzept | <input checked="" type="checkbox"/> Rechteverwaltung |
| <input checked="" type="checkbox"/> Nur notwendigste Administratoren | <input checked="" type="checkbox"/> Passwortrichtlinie |
| <input checked="" type="checkbox"/> Physische Löschung von Datenträgern | <input checked="" type="checkbox"/> Sichere Aufbewahrung von Datenträgern |
| <input checked="" type="checkbox"/> Einsatz von Aktenvernichtern bzw. Dienstleistern | <input checked="" type="checkbox"/> Ordnungsgemäße Vernichtung von Datenträgern (in Anlehnung an DIN 66399) |
| <input checked="" type="checkbox"/> Verschlüsselung von Datenträgern | <input checked="" type="checkbox"/> Protokollierung der Vernichtung |
| <input checked="" type="checkbox"/> Einsatz einer Hardware-Firewall | <input checked="" type="checkbox"/> Einsatz von Anti-Viren-Software |
| <input checked="" type="checkbox"/> Einsatz von Software-Firewall | |

4 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 vorgehen ist.

- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- Beim physischen Transport: sichere Transportbehälter/-verpackungen
- E-Mail-Verschlüsselung

5 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)

6 Auftragskontrolle

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

- Auswahl der (Unter-) Auftragsverarbeiter unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Schriftlich dokumentierte Weisungen an den Auftragsverarbeiter (z.B. über AVV)
- Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf Vertraulichkeit
- Datenschutzbeauftragten ist bestellt

7 Verfügbarkeitskontrolle

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

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleiste in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Backup- und Recoverykonzept
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Serverräume nicht unter sanitären Anlagen

8 Trennungsgebot

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

- Festlegung von Datenbank-Rechten
- Logische Mandantentrennung (Software)
- Trennung von Produktiv- und Testsystem
- Keine Produktivitätsdaten in Testsystemen



Anlage 3 Eingesetzte Unterauftragnehmer

Nr.	Name und Anschrift des Unterauftragnehmers	Beschreibung der Teilleistungen	Ort der Leistungserbringung
1			
2			

Stand 01.07.2022: Es werden keine Unterauftragnehmer eingesetzt.