Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

zwischen
dem Lizenznehmer der Katalogsysteme
- nachfolgend **„Auftraggeber“** genannt -

und
dem Unternehmen der Stahlgruber Gruppe laut Hauptvertrag
- nachfolgend **„Auftragnehmer“** genannt –

1 Geltungsbereich

1.1 Der Auftragnehmer ist ein Ersatzteilhändler, der Filialen und Standorte in Deutschland betreibt. Für die Betreuung, die Ersatzteilversorgung und Abwicklungsprozesssteuerung mit dem Auftraggeber bietet der Auftragnehmer dem Auftraggeber diverse IT-Systeme an.

1.2 Die Leistungserbringung nach dem Lizenzvertrag und den Lizenz- und Nutzungsbedingungen in der jeweils gültigen Fassung („Hauptvertrag“) bringt es mit sich, dass der Auftragnehmer Zugang zu personenbezogenen Daten des Auftraggebers erhält und diese ggf. auch verarbeitet, für die der Auftraggeber als datenschutzrechtlich Verantwortlicher fungiert („Auftraggeber-Daten“). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien bei der Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer.

1.3 Im Falle von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus diesem Vertrag vor.

2 Gegenstand und Umfang der Verarbeitung von personenbezogen Daten im Auftrag

2.1 Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag und auf Weisung des Auftraggebers im Sinne von Art. 28 Abs. 1 DSGVO (Verarbeitung im Auftrag). Der Auftraggeber bleibt im datenschutzrechtlichen Sinn Verantwortlicher.

2.2 In Anlage 1 zu diesem Vertrag ist abschließend festgelegt, welche Arten von Auftraggeber-Daten der Auftragnehmer auf welche Arten und für welche Zwecke verarbeiten darf und auf welche Kategorien betroffener Personen sich die Auftraggeber-Daten beziehen.

2.3 Die Verarbeitung der Auftraggeber-Daten findet im Gebiet eines Mitgliedstaats der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Datenverarbeitungen in anderen Ländern dürfen erfolgen, sofern der Auftraggeber die Voraussetzungen der Art. 44 bis 47 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt.

3 Umfang der Weisungsbefugnisse des Auftraggebers

3.1 Der Auftragnehmer verarbeitet die Auftraggeber-Daten gemäß den Weisungen des Auftraggebers, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.2 Die Weisungen des Auftraggebers sind grundsätzlich abschließend in den Bestimmungen dieses Vertrags festgelegt und dokumentiert. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers und erfolgen nach Maßgabe des im Hauptvertrag festgelegten Änderungsverfahrens, in dem die Weisung zu dokumentieren und die Übernahme etwa dadurch bedingter Mehrkosten des Auftragnehmers durch den Auftraggeber zu regeln ist.

3.3 Die Weisungen des Auftraggebers bedürfen grundsätzlich der Schrift- oder der Textform. Im Eilfall kann der Auftraggeber Weisungen auch mündlich oder telefonisch erteilen. Mündlich oder telefonisch erteilte Weisungen bedürfen jedoch einer unverzüglichen Bestätigung des Auftraggebers in Schrift- oder Textform.

3.4 Sämtliche Weisungen sind durch den Auftraggeber zu dokumentieren.

3.5 Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag, eine frühere Weisung oder das geltende Datenschutzrecht verstößt, wird er den Auftraggeber hierüber informieren. Der Auftragnehmer ist in diesem Fall berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen. Die Parteien stimmen darin überein, dass die alleinige Verantwortung für die weisungsgemäße Verarbeitung der Auftraggeber-Daten beim Auftraggeber liegt.

4 Pflichten und Rechtsstellung des Auftraggebers

4.1 Der Auftraggeber ist für die datenschutzrechtliche Zulässigkeit der Verarbeitung der Auftraggeber-Daten gegenüber betroffenen Personen sowie für die Wahrung der Rechte der betroffenen Personen verantwortlich. Sollten Dritte gegen den Auftragnehmer wegen einer vermeintlich unzulässigen Verarbeitung von Auftraggeber-Daten Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

4.2 Dem Auftraggeber obliegt es, dem Auftragnehmer die Auftraggeber-Daten rechtzeitig zur Leistungserbringung zur Verfügung zu stellen und er ist verantwortlich für die Qualität der Auftraggeber-Daten. Der Auftraggeber hat den Auftragnehmer unverzüglich zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich der datenschutzrechtlichen Bestimmungen oder seiner Weisungen feststellt.

4.3 Der Auftraggeber hat dem Auftragnehmer auf Anforderung die in Art. 30 Abs. 2 DSGVO genannten Angaben zur Verfügung zu stellen, soweit sie dem Auftragnehmer nicht vorliegen.

5 Anforderungen an Personal / Vertraulichkeit

Der Auftragnehmer gewährleistet, dass alle mit der Verarbeitung von Auftraggeber-Daten beschäftigten Personen schriftlich zur Wahrung der Vertraulichkeit im Hinblick auf die Auftraggeber-Daten verpflichtet wurden.

6 Sicherheit der Verarbeitung

6.1 Der Auftragnehmer verpflichtet sich, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten. Diese Maßnahmen schließen unter anderem Folgendes ein:

a) Verschlüsselung der Auftraggeber-Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der Auftraggeber-Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

6.2 Der Auftragnehmer gewährleistet, dass er die in Anlage 2 dieses Vertrags spezifizierten technischen und organisatorischen Maßnahmen ergreift und diese während der Vertragslaufzeit aufrechterhält.

6.3 Da die technischen und organisatorischen Maßnahmen dem technischen Fortschritt unterliegen, ist es dem Auftragnehmer gestattet, alternative, adäquate Maßnahmen umzusetzen, sofern dabei das Sicherheitsniveau der in dieser Ziffer festgelegten Maßnahmen nicht unterschritten wird.

7 Inanspruchnahme weiterer Auftragsverarbeiter

7.1 Der Auftragnehmer darf nach genauerer Maßgabe dieser Ziffer 7 Auftragsverhältnisse mit weiteren Auftragsverarbeitern hinsichtlich der Verarbeitung oder Nutzung von Auftraggeber-Daten begründen, ohne dass es einer gesonderten Zustimmung des Auftraggebers im Einzelfall bedarf. Die zum Zeitpunkt des Vertragsschlusses hinzugezogenen weiteren Auftragsverarbeiter ergeben sich aus Anlage 3.

7.2 Der Auftragnehmer wird alle weiteren Auftragsverarbeiter in einer schriftlichen Vereinbarung ebenso verpflichten, wie auch der Auftragnehmer aufgrund dieses Vertrags gegenüber dem Auftraggeber verpflichtet ist bzw. dem weiteren Auftragsverarbeiter die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegen.

7.3 Der Auftragnehmer wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung weiterer oder die Ersetzung von weiteren Auftragsverarbeitern vorab informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, gegen die Beauftragung eines potentiellen weiteren Auftragsverarbeiters Einspruch zu erheben. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erfolgen. Soweit der Auftraggeber innerhalb von 14 Tagen nach Zugang der Benachrichtigung nicht Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von 3 Monaten zu kündigen.

8 Rechte der betroffenen Personen

8.1 Für die Beantwortung von Anträgen auf Wahrnehmung der nach den Art. 12 ff. DSGVO bestehenden Rechte der betroffenen Personen („Betroffenenrechte“) ist der Auftraggeber zuständig.

8.2 Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer zwecks Wahrnehmung der ihr zustehenden Betroffenenrechte wenden sollte, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten.

8.3 Der Auftragnehmer wird den Auftraggeber bei der Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte im Rahmen des Erforderlichen und Zumutbaren unterstützen. Der Auftraggeber hat dem Auftragnehmer die hierdurch entstehenden Aufwände und Kosten zu ersetzen.

9 Sonstige Unterstützungspflichten des Auftragnehmers

9.1 Soweit dem Auftraggeber eine gesetzliche Melde- oder Benachrichtigungspflicht wegen einer Verletzung des Schutzes von Auftraggeber-Daten (insbesondere nach Art. 33, 34 DSGVO) trifft, wird der Auftragnehmer den Auftraggeber zeitnah über etwaige meldepflichtige Ereignisse in seinem Verantwortungsbereich informieren. Der Auftragnehmer wird den Auftraggeber bei der Erfüllung der Melde- und Benachrichtigungspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden Aufwände und Kosten unterstützen.

9.2 Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden Aufwände und Kosten bei etwa vom Auftraggeber durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

9.3 Außerdem unterstützt der Auftragnehmer den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32 DSGVO genannten Pflichten im Rahmen des Zumutbaren und Erforderlichen sowie gegen Erstattung der dem Auftragnehmer hierdurch entstehenden Aufwände und Kosten.

10 Rückgabe und Löschung von Auftraggeber-Daten

10.1 Der Auftragnehmer wird auf die Weisung des Auftraggebers hin mit Beendigung des Hauptvertrages, alle Auftraggeber-Daten entweder vollständig und unwiderruflich löschen oder an den Auftraggeber zurückgeben, sofern nicht gesetzlich eine Verpflichtung des Auftragnehmers zur weiteren Speicherung der Auftraggeber-Daten besteht.

10.2 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, dürfen durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahrt werden.

11 Nachweise und Überprüfungen

11.1 Der Auftragnehmer wird dem Auftraggeber auf dessen Anforderung alle erforderlichen und beim Auftragnehmer vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung stellen.

11.2 Der Auftraggeber ist berechtigt, den Auftragnehmer bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen; einschließlich durch Inspektionen.

11.3 Der Auftraggeber darf in der Regel eine Kontrolle pro Kalenderjahr durchführen. Weitere Überprüfungen erfolgen gegen Kostenerstattung und nach Abstimmung mit dem Auftragnehmer. Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren.

11.4 Zur Durchführung von Inspektionen nach vorstehenden Ziffern ist der Auftraggeber berechtigt, im Rahmen der üblichen Geschäftszeiten nach rechtzeitiger Vorankündigung gemäß Ziffer 11.3 auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers die Geschäftsräume des Auftragnehmers zu betreten, in denen Auftraggeber-Daten verarbeitet werden.

11.5 Der Auftragnehmer ermöglicht solche Überprüfungen und trägt durch alle zweckmäßigen und zumutbaren Maßnahmen zu solchen Überprüfungen bei; unter anderem durch die Gewährung der notwendigen Zugangs- und Zugriffsrechte und die Bereitstellung aller notwendigen Informationen.

11.6 Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Kontrollzwecke sind, zu erhalten.

11.7 Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Überprüfung, so hat er hierfür entstehenden Aufwände und Kosten selbst zu tragen. Ferner hat frt Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch den Auftraggeber aufgrund von dieser Ziffer 11 dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber ihm die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Wettbewerber des Auftragnehmers mit der Kontrolle beauftragen.

11.8 Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der Pflichten nach diesem Vertrag anstatt durch eine Inspektion auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit („Prüfungsberichts“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der vertraglichen Pflichten zu überzeugen.

11.9 Der Auftragnehmer unterstützt den Auftraggeber bei Kontrollen durch die Aufsichtsbehörde im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden, Aufwände und Kosten, soweit diese Kontrollen die Datenverarbeitung durch den Auftragnehmer betreffen.

12 Vertragsdauer und Kündigung

12.1 Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags.

12.2 Eine Kündigung des Hauptvertrages bewirkt automatisch die Kündigung dieses Vertrages. Eine isolierte Kündigung dieses Vertrages ist ausgeschlossen.

13 Schlussbestimmungen

13.1 Änderungen, Ergänzungen und die Aufhebung dieses Vertrags bedürfen der Schriftform. Gleiches gilt für eine Änderung oder Aufhebung des Schriftformerfordernisses.

13.2 Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der betreffenden unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem wirtschaftlichen Zweck der unwirksamen Regelung am nächsten kommt bzw. diese Lücke ausfüllt.

13.3 Alleiniger Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist der Sitz des Auftragnehmers, soweit kein ausschließlicher Gerichtsstand begründet ist.

gez. Auftraggeber gez. Auftragnehmer

Anlagen:

Anlage 1: Zweck und Art der Verarbeitung, Art der Daten und Kategorien betroffener Personen
Anlage 2: Technische und organisatorische Maßnahmen gemäß Ziffer 6 des Vertrages über die Verarbeitung personenbezogener Daten im Auftrag
Anlage 3: Auflistung weiterer Auftragsverarbeiter

<u>Anlage 1</u>: **Zweck und Art der Verarbeitung, Art der Daten und Kategorien betroffener Personen**

Arten der Auftraggeber-Daten	• Stamm- und Kontaktdaten von Kunden und Interessenten des Auftraggebers Daten zur Identifikation von Fahrzeugen und technische Fahrzeugdaten • Angaben zu Geschäftsvorfällen inkl. historischer Daten: insbesondere Bestellungen, Angebote, Wartungspläne, Bauteile, Arbeitswerte sowie ggf. kundenspezifische Preise und Stundensätze Nutzungsdaten • Schulungsdaten Alle vom Auftraggeber in Freitextfelder eingegebene Daten
Arten der Verarbeitung	• Verwaltung von Kundendaten und Bereitstellung für andere Module der Applikation Zugriff auf Systeme und Daten des Auftraggebers zum Zweck des Supports und der Fernwartung • Übernahme von Angaben in Freitextfeldern in Warenbegleitpapiere, Rechnungen etc. Bereitstellung von Schnittstellen zu Applikationen / Modulen Dritter
Zwecke der Verarbeitung	• Erbringung der Leistungen nach dem Hauptvertrag; insbesondere Erleichterung der Teileauswahl und der Erstellung von Angeboten- und Wartungsplänen durch Bereitstellung eines Moduls zur Verwaltung von Kunden- und Fahrzeugdaten • Erleichterung von innerbetrieblichen Abläufen des Auftraggebers durch Bereitstellung von Freitextfeldern und Übernahme der Daten in Rechnungen und Warenbegleitpapiere Unterstützung des Auftraggebers bei Anwendungsproblemen und bei allgemeinen Supportanfragen
Kategorien betroffener Personen	• Kunden, Interessenten, Mitarbeiter und Geschäftspartner des Auftraggebers Nutzer der Applikation • ggf. sonstige natürliche Personen im Rahmen von Angaben in Freitextfeldern

<u>Anlage 2:</u> **Technische und organisatorische Maßnahmen gemäß Ziffer** 6 **des Vertrages über die Verarbeitung personenbezogener Daten im Auftrag**

1 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

☒ Verarbeitung von personenbezogenen Daten in pseudonymisierter oder verschlüsselter Form

☒ Verschlüsselung der Daten bei weiteren Onlineübertragungen

☒ Verschlüsselung von Smartphone-Inhalten

2 Vertraulichkeit (Art. 32 Abs.1 lit. b DSGVO)

Zugangskontrolle

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle)

☒ Chipkarten-/Transponder-Schließsystem

☒ Manuelles Schließsystem

☒ Sicherheitsschlösser

☒ Schlüsselregelung (Schlüsselausgabe etc.)

☒ Personenkontrolle beim Pförtner / Empfang

☒ Protokollierung der Besucher

☒ Tragepflicht von Berechtigungsausweisen (Besucher)

☒ Sorgfältige Auswahl von Reinigungspersonal

☒ Sorgfältige Auswahl von Wachpersonal

Benutzerkontrolle

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle)

☒ Zuordnung von Benutzerrechten

☒ Erstellen von Benutzerprofilen

☒ Passwortvergabe

☒ Authentifikation mit Benutzername / Passwort

☒ Zuordnung von Benutzerprofilen zu IT-Systemen

☒ Einsatz von VPN-Technologie

☒ Sicherheitsschlösser

☒ Einsatz von Intrusion-Detection-Systemen

☒ Verschlüsselung von Smartphone-Inhalten

☒ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)

☒ Einsatz von Anti-Viren-Software

☒ Einsatz einer Hardware-Firewall

Zugriffs- und Datenträgerkontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle) und Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle)

- ☒ 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)
- ☒ Verwaltung der Rechte durch Systemadministrator
- ☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- ☒ Sichere Aufbewahrung von Datenträgern
- ☒ ordnungsgemäße Vernichtung von Datenträgern (etwa DIN 66399)
- ☒ Protokollierung der Vernichtung

Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit)

- ☒ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern für HR-Daten
- ☒ Erstellung eines Berechtigungskonzepts
- ☒ Festlegung von Datenbankrechten
- ☒ Logische Mandantentrennung (softwareseitig)
- ☒ Trennung von Produktiv- und Testsystem

3 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Übertragungs- und Transportkontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle) und dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle)

- ☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☒ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☒ Automatische Überwachung auf Unregelmäßigkeiten und Echtzeitanalysen von Systemalarmen (SIEM)
- ☒ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- ☒ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen

Eingabe- und Speicherkontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle) und Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle)

- ☒ Protokollierung der Eingabe, Änderung und Löschung von Daten; Aufbewahrung der Protokolle
- ☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- ☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☒ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

4 Verfügbar- und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeit

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)

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

Belastbarkeit der Systeme

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität)

- ☒ Regelmäßige Überprüfung der Betriebsbereitschaft aller Funktionen der Systeme
- ☒ Regelmäßige Wartung der Systeme
- ☒ Automatisierte Meldung von Fehlfunktionen
- ☒ Funktionale Trennung zwischen IT-Abteilung und anderen Abteilungen
- ☒ Virenschutz
- ☒ Firewalls
- ☒ Durchführung einer Risiko- und Schwachpunktanalyse
- ☒ Ständige Aktualisierung der genutzten Software

5 Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Art. 32 Abs. 1 lit. c DSGVO)

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit)

- ☒ Erstellung von Sicherheitskopien in regelmäßigen Abständen
- ☒ Speicherung der Sicherheitskopien an einem sicheren Ort außerhalb der IT-Abteilung
- ☒ Prüfung der Wiederherstellungsfähigkeit der Sicherheitskopien in regelmäßigen Abständen
- ☒ Datenwiederherstellungsprozeduren
- ☒ Datenspiegelungen
- ☒ Aufstellung von Servern in separierten und gesichertem Serverraum oder einem Rechenzentrum
- ☒ Gewährleistung der Aktualität der Sicherungskopien, Rhythmus der Sicherung und des Mediums:
- ☒ Festgelegte Aufbewahrungszeit der Sicherungskopien

6 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d, 25 Abs. 1 DSGVO)

Auftragskontrolle

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle)

- ☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☒ vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- ☒ schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. Art. 28 Abs. 3 DSGVO
- ☒ Schriftliche Verpflichtung der Mitarbeiter des Auftragnehmers zur Vertraulichkeit
- ☒ Auftragnehmer hat Datenschutzbeauftragten bestellt sofern erforderlich
- ☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☒ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- ☒ laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

Datenschutz-Management

- ☒ Vorliegen eines Datensicherheitskonzepts
- ☒ Überprüfung der Datenverarbeitungssysteme und -programme nach Industriestandards
- ☒ Bestehen eines Verzeichnisses von Verarbeitungstätigkeiten
- ☒ Vorhandenes Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der ergriffenen der technischen und organisatorischen Maßnahmen (etwa Penetrationstests)

Datenschutzfreundliche Voreinstellungen

- ☒ Aktualisierung der Datenverarbeitung nach dem Stand der Technik
- ☒ Pseudonymisierung der Datensätze

Incident-Response-Management

- ☒ Dokumentiertes Incident-Response-Management
- ☒ Standardisierte Verfahren für die Ergreifung von unmittelbaren Schutzmaßnahmen
- ☒ Vollständige und umfassende Dokumentation des Vorfalls und der ergriffenen Maßnahmen

<u>Anlage 3</u>: Auflistung weiterer Auftragsverarbeiter

Name	**Anschrift**	**Einsatzzweck/vom weiteren Auftragsverarbeiter erbrachte Leistungen**	**Vom weiteren Auftragsverar-beiter verarbeitete Arten personenbezogener Daten**
Absolute Software GmbH	Jungfernstieg 49 20354 Hamburg Deutschland	Bereitstellung und Support Contenmarketingmodul PV:WELT, Bonusprogramm PV:PLUS, Trainingsmodul PV:TRAINING, Modulstore, Autofahrer App, Administrationstool für Webseiten AUTOFIT und meinewerkstatt	Personenstammdaten, Kommunikationsdaten, Vertragsstammdaten, Auftragnehmerereigene Stammdaten, Fahrzeugdaten
DVSE GmbH	Carl-Benz-Weg 1 22941 Bargteheide Deutschland	Bereitsstellung und Support Katalog- und Informationssystem	Personenstammdaten, Kommunikationsdaten, Vertragsstammdaten, Händlereigene Stammdaten, Fahrzeugdaten
Euro Car Parts Limited	T2 Birch Coppice Business Park, Danny Morson Way, Dordon, Tamworth, England, B78 1SE	Bereitstellung LKQ Academy	Personenstammdaten, Kommunikationsdaten, Vertragsstammdaten, Schulungsdaten
Jfnetwork GmbH	Steigweg 24 97018 Kitzingen Deutschland	Bereitstellung des Räderkonfigurator	Personenstammdaten, Fahrzeugdaten, Kommunikationsdaten
Limex Computer GmbH	Holsten-Mündruper Straße 80 49086 Osnabrück Deutschland	Bereitsstellung und Support Dealer-Management-System	Personenstammdaten, Kommunikationsdaten, Vertragsstammdaten, Auftragnehmerereigene Stammdaten, Fahrzeugdaten