VERTRAG ZUR DATENVERARBEITUNG GEMÄSS ARTIKEL 28 (3) EU-DATENSCHUTZGRUNDVERORDNUNG (EU-DS GVO)

Dieser Datenschutzvertrag (der »Anhang«) wird zwischen den untenstehenden Gesellschaften getroffen:

Kundenbezeichnung, Adresse

(1)

– nachfolgend als »Verantwortlicher« bezeichnet –

(2) WM SE, Pagenstecherstraße 121, D-49090 Osnabrück

– nachfolgend als »Auftragsverarbeiter« bezeichnet –

Sowohl der Verantwortliche als auch der Auftragsverarbeiter können gemeinsam auch als »die Parteien« bzw. jeder Einzelne als »die Partei« bezeichnet werden.

VORWORT

Artikel 28 der EU-DS GVO vom 27. April 2016 kommt mit Wirkung zum 25. Mai 2018 auf die Verarbeitung von personenbezogenen Daten in der Europäischen Union und dem Europäischen Wirtschaftsraum zur Anwendung, um ausreichende technische und organisatorische Schutzmaßnahmen bei der Verarbeitung personenbezogener Daten des Verantwortlichen durch einen Auftragsverarbeiter zu garantieren.

Dieser Anhang spezifiziert die Verpflichtungen der Parteien bezüglich der Verarbeitung personenbezogener Daten auf Anweisung des Verantwortlichen. Es besteht Einvernehmen zwischen den Vertragsparteien, dass die Vereinbarungen für beide Parteien in allen wechselseitigen Vertragsbeziehungen rechtsverbindlich sind.

Dauer und Zweck des Verarbeitungsauftrags, Kategorien zu verarbeitender personenbezogener Daten und von der Verarbeitung Betroffene sind in Anlage 1 zu diesem Anhang aufgelistet.

1 DEFINITIONEN UND AUSLEGUNGEN

1.1 DEFINITIONEN

Sofern nicht ausdrücklich anders festgelegt, haben die Begriffe in diesem Anhang folgende Bedeutung:

»Datenschutzgesetze« meinen die Datenschutzgesetze am Hauptsitz des Verantwortlichen (inklusive der EU-DS GVO vom 27. April 2016) und alle Datenschutzgesetze, die auf den Verantwortlichen im Zusammenhang mit dem Hauptvertrag zur Anwendung kommen können.
»Personenbezogene Daten« sind Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden »betroffene Person«) beziehen, deren Daten im Auftrag des Verantwortlichen durch den Auftragsverarbeiter im Rahmen des Hauptvertrages verarbeitet werden.
»Verarbeitung« bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang 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, Verarbeitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
»Technische und organisatorische Schutzmaßnahmen« bezeichnen Maßnahmen zum Schutz personenbezogener Daten gegen versehentliche oder vorsätzliche Zerstörung, Verlust, Änderung, unbefugte Weitergabe oder Zugriff und gegen alle anderen rechtswidrigen Formen der Verarbeitung.
»Verletzung des Schutzes personenbezogener Daten« bedeutet eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet werden.
»Schriftlich« beinhaltet auch die elektronische Form.

1.2 AUSLEGUNGEN

Im Falle von Änderungen oder Ersatz von Datenschutzgesetzen, auf die im vorliegenden Anhang referenziert wird, gelten die neuen gesetzlichen oder begrifflichen Änderungen, sobald sie in Kraft getreten sind und zur Anwendung kommen.

2 PFLICHTEN DES AUFTRAGVERARBEITERS

2.1 ANWEISUNGEN

2.1.1 Der Auftragsverarbeiter hat die personenbezogenen Daten jederzeit in Übereinstimmung mit diesem Anhang (insbesondere mit Anlage 1 dieses Anhangs) und dem Hauptvertrag zu verarbeiten. Die personenbezogenen Daten dürfen nur zu dem im Hauptvertrag und zu weiteren mit diesem Vertrag zusammenhängenden Anweisungen des Verantwortlichen genannten Zweck verarbeitet werden. Der Auftragsverarbeiter muss eine aktuelle, vollständige und genaue Aufzeichnung aller Anweisungen führen.

2.1.2 Sofern der Auftragsverarbeiter die personenbezogenen Daten aufgrund zwingender gesetzlicher Vorschriften verarbeiten muss, ist der Verantwortliche hierüber vor Beginn der Verarbeitung schriftlich zu informieren, es sei denn, das Gesetz verbietet die Veröffentlichung dieser Information aus wichtigen Gründen des öffentlichen Interesses. In diesem Fall hat der Auftragsverarbeiter den Verantwortlichen unmittelbar und ohne Verzug zu informieren, sobald die Veröffentlichung der Information gesetzlich erlaubt ist.

2.1.3 Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich schriftlich zu informieren, sobald er der Ansicht ist, eine Anweisung des Verantwortlichen würde gegen Datenschutzgesetze verstoßen und hat dies detailliert und schriftlich zu begründen. Bei Anzweiflung der Rechtmäßigkeit einer Anweisung hat der Auftragsverarbeiter geeignete Untersuchungen einzuleiten.

2.1.4 Der Auftragsverarbeiter muss einen Datenschutzbeauftragten ernennen und dem Verantwortlichen auf Verlangen dessen Kontaktdaten übermitteln.

2.2 TECHNISCHE UND ORGANISATORISCHE SCHUTZMASSNAHMEN

2.2.1 Der Auftragsverarbeiter garantiert die Implementierung angemessener technischer und organisatorischer Schutzmaßnahmen in der Art, dass die Verarbeitung den Anforderungen der Datenschutzgesetze genügen und die Rechte der Betroffenen bezüglich Datenschutzanforderungen sichergestellt und gewahrt werden.

2.2.2 Unter Berücksichtigung von Stand der Technik, Art, Umfang, Kontext und Zweck der Verarbeitung und unter Berücksichtigung der Risiken für die Rechte und Freiheiten betroffener natürlicher Personen implementiert der Auftragsverarbeiter angemessene technische und organisatorische Schutzmaßnahmen, in jedem Fall aber mindestens die in Anlage 2 dieses Anhangs dokumentierten Maßnahmen.

2.2.3 Der Auftragsverarbeiter ist verpflichtet, die technischen und organisatorischen Schutzmaßnahmen laufend zu monitoren, zu testen, sie regelmäßig zu überprüfen und auf ihre Effektivität hin zu beurteilen. Die technischen und organisatorischen Schutzmaßnahmen sind durch den Auftragsverarbeiter kontinuierlich zu verbessern. Bei Änderungen an den technischen und organisatorischen Schutzmaßnahmen und auf Anfrage ist dem Verantwortlichen eine aktualisierte Version von Anlage 2 dieses Anhangs zu übergeben.

2.2.4 Der Auftragsverarbeiter hat seine technischen und organisatorischen Schutzmaßnahmen zu dokumentieren und dem Verantwortlichen auf Anfrage zu überreichen.

2.3 ANFORDERUNGEN AN DAS PERSONAL

Der Auftragsverarbeiter stellt sicher, dass die mit der Verarbeitung der personenbezogenen Daten befassten Personen auf Verschiegenheit verpflichtet wurden oder einer entsprechenden gesetzlichen Verschwiegenheitspflicht unterliegen und die personenbezogenen Daten nur entsprechend der in diesem Anhang dokumentierten Anweisungen verarbeiten. Er hat sicherzustellen, dass die mit der Verarbeitung der personenbezogenen Daten befassten Personen angemessene Schulungen erhalten und ihre Verantwortung in Bezug auf Datenschutz im Verarbeitungsprozess verstanden haben.

2.4 VERTRAULICHKEIT

Der Auftragsverarbeiter stimmt zu, dass er die personenbezogenen Daten vertraulich behandeln muss. Insbesondere stimmt der Auftragsverarbeiter zu, dass er keine ihm überlassenen personenbezogenen Daten ohne vorherige Zustimmung des Verantwortlichen an Dritte weitergeben darf, es sei denn, er ist aufgrund zwingender gesetzlicher Vorschriften hierzu verpflichtet. Ist der Auftragsverarbeiter verpflichtet, personenbezogene Daten an eine Strafverfolgungsbehörde oder an Dritte weiterzugeben, hat er dies dem Verantwortlichen vor Gewährung des Zugriffs in angemessener Form mitzuteilen, so dass der Verantwortliche noch vor dem Zugriff erlaubte Rechtsmittel einsetzen kann. Ist die Mitteilung einer Zugriffsanfrage aus gesetzlicher Sicht verboten, ist der Auftragsverarbeiter verpflichtet, seinerseits alle zulässigen Maßnahmen zu ergreifen, um die personenbezogenen Daten vor unberechtigter Offenlegung zu schützen. Er hat dabei so zu handeln, als wäre er selber Verantwortlicher. Sobald das gesetzliche Verbot über die Mitteilung der Zugriffsanfrage nicht mehr gilt, hat er den Verantwortlichen unverzüglich über die Anfrage zu informieren.

2.5 RECHTE DER BETROFFENEN

2.5.1 Bei Eingang einer Beschwerde oder einer Anfrage zur Verarbeitung der personenbezogenen Daten oder zur Einhaltung der Datenschutzgesetze im Zusammenhang mit der Verarbeitung, antwortet der Auftragsverarbeiter nicht, sondern benachrichtigt den Verantwortlichen unverzüglich. Der Auftragsverarbeiter arbeitet in einem solchen Fall uneingeschränkt mit dem Verantwortlichen zusammen und stellt erforderliche Informationen zur Verfügung einschließlich, aber nicht beschränkt auf die Korrektur, Löschung und Sperrung personenbezogener Daten. Der Auftragsverarbeiter muss geeignete technische und organisatorische Maßnahmen ergreifen, um bei einer solchen Anfrage behilflich zu sein.

2.5.2 Im Falle eines Antrags eines Betroffenen antwortet der Auftragsverarbeiter dem Betroffenen nicht, sondern informiert den Verantwortlichen umgehend und unterstützt ihn bei der Bearbeitung des Antrags.

2.6 UNTERSTÜTZUNG BEI DER EINHALTUNG GESETZLICHER VORSCHRIFTEN

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung der Verpflichtungen gemäß Artikel 28 (3) f EU-DS GVO, einschließlich Unterstützung in Bezug auf:

(a) Datenschutz-Folgenabschätzung, durch Bereitstellung von Informationen und Unterstützungsleistungen, die der Verantwortliche zur Durchführung der Datenschutz-Folgenabschätzung, zur regelmäßigen Überprüfung und zur Bewertung der implementierten Schutzmaßnahmen benötigt;

(b) vorherige Konsulation einer Datenschutzaufsichtsbehörde bezüglich der Hochrisikoverfahren.

2.7 COMPLIANCE, INFORMATIONEN UND AUDITS

Auf Anfrage des Verantwrtlichen stellt der Auftragsverarbeiter dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der in diesem Anhang festgelegten Pflichten erforderlich sind. Nach Einhaltung einer angemessenen Frist lässt der Auftragsverarbeiter auf Anweisung des Verantwortlichen Prüfungen zu (einschließlich entsprechender Prüfungen vor Ort), die vom Verantwortlichen selber, von einem verbundenen Unternehmen oder einem Dritten durchgeführt werden. Der Verantwortliche kann die Einhaltung der Bestimmungen dieses Anhangs bis zu zweimal jährlich sowie bei Verdacht auf Vertragsbruch oder Verletzung personenbezogener Daten prüfen.

2.8 AUFZEICHNUNGEN

Der Auftragsverarbeiter muss vollständige, genaue und aktuelle schriftliche Aufzeichnungen über die im Auftrag des Verantwortlichen durchgeführten Verarbeitungstätigkeiten führen und diese dem Verantwortlichen auf Verlangen zur Verfügung stellen.

2.9 UNTERBEAUFTRAGUNG

2.9.1 Der Auftragsverarbeiter darf keine seiner Rechte oder Pflichten aus diesem Anhang ohne vorherige schriftliche Zustimmung des Verantwortlichen übertragen. Der Verantwortliche stimmt der Untervergabe der Verarbeitungstätigkeiten durch den Auftragsverarbeiter an die in Anhang 3 aufgeführten Unterauftragnehmer zu.

2.9.2 Übergibt der Auftragsverarbeiter mit Zustimmung des Verantwortlichen seine Pflichten aus dieser Anlage einem Unterauftragnehmer, hat er hierzu einen verbindlichen schriftlichen Vertrag mit dem Unterauftragnehmer zu schließen, der diesem die gleichen Verpflichtungen insbesondere hinsichtlich der Anweisungen zu Personal und zu technischen und organisatorischen Maßnahmen auferlegt. Zur Vermeidung von Zweifeln hat der Verantwortliche auch gegenüber dem Unterbeauftragten die in Abschnitt 2.7 festgelegten Rechte in Bezug auf Unterstützung und Prüfungen. Der Auftragsverarbeiter übermittelt dem Verantwortlichen den Namen und die Adresse des Unterauftragnehmers und auf Antrag auch eine Kopie der Unterauftragsvereinbarung.

2.9.3 Wenn die Anweisungen des Auftragverarbeiters mit denen des Verantwortlichen in Konflikt stehen, bestätigt der Auftragsverarbeiter, dass die Anweisungen des Verantwortlichen Vorrang vor denen des Auftragsverarbeiters haben.

2.9.4 Wenn der Unterauftragnehmer seinen Datenschutzverpflichtungen aus einem Untervertrag oder aus Datenschutzgesetzen nicht nachkommt, bleibt der Auftragsverarbeiter dem Verantwortlichen in vollem Umfang haftbar für die Erfüllung seiner Verpflichtungen aus diesem Anhang und für die Erfüllung der Verpflichtungen des Unterauftragnehmers.

2.10 INTERNATIONALER DATENAUSTAUSCH

2.10.1 Die personenbezogenen Daten werden ausschließlich in einem Mitgliedstaat der Europäischen Union (»EU-Mitgliedstaat«) oder in einem anderen Unterzeichnerstaat des Abkommens über den Europäischen Wirtschaftsraum ("EWR-Länder") verarbeitet und genutzt.

2.10.2 Wenn der für die Verarbeitung Verantwortliche der internationalen Übermittlung personenbezogener Daten in ein Land schriftlich zustimmt, das weder ein EU-Mitgliedstaat noch ein EWR-Land ist oder an eine internationale Organisation oder wenn der Auftragsverarbeiter außerhalb der Europäischen Union oder außerhalb des Europäischen Wirtschaftsraums niedergelassen ist oder wenn es sich bei ihm um eine internationale Organisation handelt, gilt Folgendes, sofern es nicht ausdrücklich schriftlich anders vereinbart ist:

(a) Die Standardvertragsklauseln der Kommision der Europäischen Union gelten für personenbezogene Daten, die vom Verantwortlichen stammen (der für die Zwecke der Standardvertragsklauseln als »Datenexporteur« gilt) und vom Auftragsverarbeiter verarbeitet werden (der für die Zwecke der Standardvertragsklauseln als »Datenimporteur« gilt) oder vom Unterauftragnehmer des Auftragsverarbeiters außerhalb des Europäischen Wirtschaftsraumes verarbeitet werden. Bei Widersprüchen zwischen den Standardvertragsklauseln und diesem Anhang haben die Standardvertragsklauseln Vorrang.

(b) Bei Ersetzung durch die Europäische Kommission können die Standardvertragsklauseln auf Antrag des Verantwortlichen ersetzt werden. In diesem Fall vereinbaren die Parteien neue Standardvertragsklauseln gemäß Artikel 26 (2) c) oder d) EU-DS GVO für die Übermittlung perso- nenbezogener Daten an Auftragsdatenverarbeiter in Drittländern.

(c) Wenn und solange die personenbezogenen Daten in ein Land übertragen und dort verarbeitet werden, für das eine Angemessenheitsentscheidung nach Art. Art. 25 (6) der Richtlinie 95/46 / EG oder Art. 45 (3) DS GVO (»Angemessenheitsbeschluss«) gilt, sind keine Standardvertragsklauseln erforderlich und gelten daher nicht für die Parteien.

2.11 BENACHRICHTIGUNG BEI VERLETZUNGEN PERSONENBEZOGENER DATEN

In Bezug auf Verletzungen personenbezogener Daten (tatsächliche oder verdächtige) muss der Auftragsverarbeiter:

(a) den Verantwortlichen und gegebenenfalls involvierte Unterbeauftragte unverzüglich (jedoch nicht später als 36 Stunden nach Kenntniserlangung der Verletzung personenbezogener Daten) über die Verletzung informieren und ihm in angemessener Weise Einzelheiten über die Verletzung mitteilen (so früh wie möglich, aber nicht später als 36 Stunden) und / oder

(b) angemessene Zusammenarbeit und Unterstützung des für die Verarbeitung Verantwortlichen in Bezug auf Maßnahmen, die im Zusammenhang mit den Verletzung gegen personenbezogene Daten im Rahmen der geltenden Datenschutzgesetze gelten, anbieten. Dies schließt auch, aber nicht ausschließlich, Maßnahmen in Bezug auf die Weitergabe des Verstoßes gegen personenbezogene Daten an die betroffenen Personen und die nationalen Datenschutzbehörden ein.

2.12 DURCHSUCHUNGEN UND BESCHLAGNAHME

Werden personenbezogene Daten durchsucht und beschlagnahmt, einem Pfändungsbeschluss, einer Einziehung während eines Konkurs oder Insolvenzverfahrens oder ähnlichen Ereignissen oder Maßnahmen durch Dritte im Verantwortungsbereich des Auftragsverarbeiters unterzogen, hat dieser den Verantwortlichen unverzüglich hierüber zu informieren. Der Auftragsverarbeiter muss bei einer solchen Aktion unverzüglich allen betroffenen Parteien mitteilen, dass alle davon betroffenen personenbezogenen Daten im alleinigen Eigentum und Verantwortungsbereich des Verantwortlichen liegen, dass die personenbezogenen Daten ausschließlich zu seiner Disposition stehen und dass der Verantwortliche zuständige Stelle gemäß der relevanten Datenschutzgesetze ist.

3 HAFTUNG

Der Auftragsverarbeiter haftet für alle Kosten, Ansprüche oder Schäden, die durch Verstöße des Auftragsverarbeiters, seines Personals oder von ihm bestellte Unterbeauftragte gegen Bestimmungen dieses Anhangs oder gegen geltende Datenschutzgesetze entstanden sind.

Für Datenverlust nicht haftbar gemacht werden kann er für die Einrichtung der Datensicherung, die eigentlich Aufgabe des Verantwortlichen ist und nur im Ausnahmefall und auf ausdrücklichen Wunsch des Verantwortlichen durch den Auftragsverarbeiter eingerichtet wurde.

4 VERTRAGSDAUER UND -BEENDIGUNG, LÖSCHUNG UND RÜCKGABE PERSONENBEZOGENER DATEN

4.1 Dieser Anhang wird mit Datum der Unterzeichnung wirksam. Unterzeichnen die Parteien an unterschiedlichen Tagen, wird der Anhang mit Datum der zuletzt gegebenen Unterschrift wirksam.

4.2 Der Anhang bleibt so lange in Kraft und wirksam, wie der Bearbeiter personenbezogene Daten im Rahmen des Hauptvertrags verarbeitet. Die Geheimhaltungsverpflichtungen des Auftragsverarbeiters bleiben auch nach Beendigung der Verpflichtungen aus diesem Anhang bestehen.

4.3 Falls der Auftragsverarbeiter wesentliche Bestimmungen aus diesem Anhang verletzt, hat der Verantwortliche das Recht, diesen Anhang sowie den Hauptvertrag aus wichtigem Grund ganz oder teilweise ohne Einhaltung einer Kündigungsfrist zu kündigen.

4.4 Nach Beendigung der Verpflichtungen aus diesem Anhang hat der Auftragsverarbeiter auf Anweisung des Verantwortlichen:

(a) alle sonstigen zwischen den Parteien getroffenen Vereinbarungen über die Rückgabe oder Vernichtung von Daten einzuhalten oder

(b) alle persönlichen Daten zurückzusenden, die der Verantwortliche zur Verarbeitung an den Auftragsverarbeiter weitergeleitet hat oder

(c) nach Erhalt der Anweisungen des Verantwortlichen alle diese Daten und ihre Kopien in einer Weise zu vernichten, die den Anforderungen der Datenschutzgesetze zur Löschung entspricht, sofern dies nicht durch geltendes Recht untersagt ist. Wenn dies der Fall ist, muss der Auftragsverarbeiter den Verantwortlichen über eine solche Anforderung informieren, sofern und solange diese Informationspflicht nicht durch geltendes Recht verboten ist.

5 VERSCHIEDENES

5.1 Im Falle eines Widerspruchs haben die Bestimmungen dieses Anhangs Vorrang vor den Bestimmungen des Hauptvertrags. Wenn einzelne Bestimmungen dieses Anhangs ungültig oder nicht durchsetzbar sind, bleiben die Gültigkeit und Durchsetzbarkeit der anderen Bestimmungen dieses Anhangs unberührt.

5.2 Alle Kosten des Auftragsverarbeiters, die sich aus der Erfüllung seiner Verpflichtungen gemäß dieses Anhangs ergeben, sind vom Auftragsverarbeiter zu tragen.

5.3 Dieser Anhang unterliegt den nationalen Gesetzen des Landes, in dem der Verantwortliche ansässig ist, und wird entsprechend ausgelegt.

Die folgenden Anlagen sind integraler Teil dieses Anhangs:
Anlage 1: Beschreibung der Verarbeitung
Anlage 2: Technische und organisatorische Schutzmaßnahmen
Anlage 3: Unterbeauftragungen

Verantwortlicher	**Auftragsverarbeiter**
vertreten durch:	vertreten durch: WM TROST
Name:	WMSE Pagenstecherstraße 121 · 49090 Osnabrück Tel. +49 541 9989-0 · Fax +49 541 1215-200 info@wm.de · www.wm.de
Titel:	**Ralf Kuhne** — **Ralf Reuwer**

ANLAGE 1: BESCHREIBUNG DER VERARBEITUNG

Sofern die Standardvertragsklauseln der Kommision der Europäischen Union zur Anwendung kommen:
Der Datenexporteuer ist gleichzusetzen mit dem “Verantwortlichen” in diesem Anhang.
Der Datenimporteur ist gleichzusetzen mit dem “Auftragsverarbeiter” in diesem Anhang.

1. DAUER DER VERARBEITUNG

Die Verarbeitung personenbezogener Daten beginnt und endet wie folgt:	
Start	Die Verarbeitung startet mit Datum der Unterzeichnung durch beide Partner.
Ende	Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Seiten jederzeit mit einer Frist von einem Monat zum Monatsende gekündigt werden. Die Möglichkeit zur außerordenltichen beziehungsweise einvernehmlichen Kündigung aus wichtigem Grund bleibt unberührt. Die Kündigung bedarf der Schriftform. Die Verpflichtung zur Geheimhaltung besteht über das Vertragsende hinaus. Die sonstigen Verpflichtungen auf dieser Vereinbarung enden mit Beendigung des Hauptvertrags.

2. KATEGORIEN VON BETROFFENEN

Folgende Personenkategorien sind von der Verarbeitung ihrer personenbezogenen Daten betroffen:

☒ Mitarbeiter
☒ Geschäftskunden
☒ Endkunden
☐ Besucher der Webseiten
☐ Newsletter-Empfänger
☐ Sonstige [bitte eintragen]

3. ZWECK DER VERARBEITUNG

Die Verarbeitung verfolgt folgende Ziele:	
☒ Mitarbeiter	☐ interne Berichtsstruktur innerhalb konzernweiter, gesellschaftenübergreifender Teams ☐ Mitarbeiterentwicklung ☐ Bonus- und Gehaltsauszahlung ☐ Zeiterfassung ☒ Bei Partnervereinbarungen: Herstellung des Kontakts ☒ Bei Nutzern der WM SE-Software (ERP und Kalkulation): IT-Support
☒ Geschäfts-kunden	☐ Zusendung von Produkten ☐ Serviceangebot (z.B. Hotline) ☐ Durchführung gemeinsamer Veranstaltungen (z.B. Messen) ☒ Bei Partnervereinbarungen: Herstellung des Kontakts ☒ Bei Nutzern der WM SE-Software (ERP und Kalkulation): IT-Support ☒ Bei Nutzern des Diagnoseportals WM ID Remote: Elektronische Fahrzeugdiagnose über Herstellerportale
☒ Endkunden	☐ Zusendung von Produkten ☐ Serviceangebot (z.B. Hotline) ☐ Marketing (z.B. Newsletter) ☒ Bei Partnervereinbarungen: Herstellung des Kontakts ☒ Bei Nutzern der WM SE-Software (ERP und Kalkulation): IT-Support ☒ Bei Nutzern des Diagnoseportals WM ID Remote: Elektronische Fahrzeugdiagnose über Herstellerportale
☐ Sonstige	[bitte eintragen]

4. KATEGORIEN PERSONENBEZOGENER DATEN

Folgende Kategorien personenbezogener Daten werden verarbeitet:

☒ Mitarbeiter	☒ Name ☒ Geschäftliche Kontaktdaten (z.B. Lokation, Telefon-Nr., Fax-Nr., E-Mail) ☐ Private Kontaktdaten (z.B. Lokation, Telefon-Nr., Fax-Nr., E-Mail) ☐ Bankverbindung und Kontodaten ☐ Auszahlungsrelevante Daten (z.B. für Gehälter, Bonuszahlungen) ☐ Leistungsbezogene Daten (z.B. Dauer Auftragsbearbeitung, Skillprofile, Anzahl Besucher am Messestand) ☒ Bei Nutzern der WM SE-Software (ERP und Kalkulation) theoretisch alle im System befindlichen Daten -> IT-Support ☒ Bei Nutzern des Diagnoseportals WM ID Remote: Referenznummer zur Identitätsprüfung (IDnow-Token)
☒ Geschäfts-kunden	☒ Geschäftliche Kontaktdaten (z.B. Adresse, Telefon-Nr., Fax-Nr., E-Mail) ☐ Private Kontaktdaten (z.B. Lokation, Telefon-Nr., Fax-Nr., E-Mail) ☐ Umsätze ☐ Produktsortiment ☒ Bei Nutzern der WM SE-Software (ERP und Kalkulation) theoretisch alle im System befindlichen Daten ☒ Bei Nutzern des Diagnoseportals WM ID Remote: Fahrzeugidentifikationsnummern und amtliche Kennzeichen der Werkstattkunden, Fahrzeugdaten in Bild und Ton
☒ Endkunden	☒ Private Kontaktdaten (z.B. Adresse, Telefon-Nr., Fax-Nr., E-Mail) ☐ Umsätze ☐ Produktsortiment ☒ Bei Nutzern der WM SE-Software (ERP und Kalkulation) theoretisch alle im System befindlichen Daten ☒ Bei Nutzern des Diagnoseportals WM ID Remote: Elektronische Fahrzeugdiagnose von Werkstattkunden über Herstellerportale, Fahrzeugdaten in Bild und Ton
☐ Sonstige	[bitte eintragen]

5. SENSITIVE DATEN

Folgende sensitive Daten werden verarbeitet:

☐ Gesundheitsdaten
☐ Genetische Daten
☐ Biometrische Daten
☐ Daten zur rassischen und ehtnischen Herkunft
☐ Daten über politische Meinungen
☐ Daten zu religiösen oder weltanschaulichen Überzeugungen
☐ Daten über die Gewerkschaftzugehörigkeit
☐ Daten zum Sexualleben oder zur sexuellen Orientierung

6. VERARBEITUNGSSCHRITTE

Die übermittelten personenbezogenen Daten werden in folgenden Basisschritten verarbeitet:

☒ Aufnahme und Speicherung der Basisdaten für Teilnahme am Partnerservice
☒ Übermittlung der Daten an den betroffenen Partner
☒ Teilweise Übermittlung von Umsätzen an Partner (gilt nur für Verantwortliche des Bosch Car Service, von Auto Crew oder Bosch-Modul-Partnern)
☒ Gegebenenfalls Unterstützung bei der Migration der Daten auf die ERP-Software
☒ Gegebenenfalls Support bei Updates und im Fehlerfall (auch über Fernwartung)
☒ Gegebenenfalls Übermittlung von technischen Fahrzeugdaten bei Nutzung des Diagnoseportals WM ID Remote.

ANLAGE 2: TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Der Auftragsverarbeiter hat ein Sicherheitsniveau zu wählen, das den Risiken der Verarbeitung für die Rechte und Freiheiten natürlicher Personen entspricht, die insbesondere durch die Verarbeitung unter anderem durch zufällige oder rechtswidrige Zerstörung, Verlust, Veränderung, unbefugte Weitergabe von oder den Zugang zu personenbezogenen Daten entsteht.
Die folgende nicht erschöpfende Liste der technischen und organisatorischen Maßnahmen, die vom Auftragsverarbeiter gemäß Abschnitt 2.2 der Anlage durchgeführt werden müssen, enthält noch keine besonderen Anforderungen in Bezug auf die Pflichten des Verantwortlichen, z.B. in Bezug auf das Recht auf Datenübertragbarkeit oder die Privatsphäre durch Design und Standard-Prinzipien. Aufgrund solcher Verpflichtungen kann der Verantworltiche den Auftragsverarbeiter anweisen, zusätzliche technische und organisatorische Maßnahmen zu ergreifen.

1. GENERELLE KONZEPTE, VERARBEITUNGEN UND PROZESSE

Der Auftragsverarbeiter muss Richtlinien zur Datensicherheit sowie spezifische Prozesse, Richtlinien, Werkzeuge und Verfahren festlegen, die erforderlich sind, um die erforderlichen und vereinbarten technischen und organisatorischen Maßnahmen umzusetzen, zu bewerten und zu aktualisieren.

Die folgenden Maßnahmen sind beim Auftragsverarbeiter umgesetzt:

- [x] Authorisierungskonzept nach dem Prinzip, Zugriff nur auf diejenigen personen-bezogenen Daten zu erhalten, die für die Aufgabenerfüllung zwingend erforderlich sind (einschließlich z.B. Verteiler, Geltungsbereich und Sicherheitszonen mit unterschiedlichem Schutzniveau)
- [x] Klare Zuordnung von Verantwortlichkeiten und ihre Kommunikation zum Personal
- [x] Effektives Sicherheitskonzept und Risikomanagement (z. B. Implementierung von Risikobeurteilungsprozessen)
- [x] Stärkung des Bewusstseins für Bedrohungen (z. B. Penetrationstests)
- [x] Change- und Release-Management (Anforderung von z. B. regulären Patches, Aktualisierungen von Systemen, Konzepten, Prozessen, Richtlinien)
- [x] Sicherstellung des Produktionsbetriebes während der Durchführung von Wartungsmaßnahmen
- [x] Implementierung von Überwachungsmechanismen zum revisionssicheren Protokollieren und Aufzeichnen von Zugriffen
- [x] Schaffung von Bedingungen zur Ermöglichung und Erleichterung interner (und externer) Audits der technischen und organisatorischen Maßnahmen einschließlich ihrer Dokumentationsanforderungen, Aufzeichnungen und Audit-Trails
- [x] Event-Management, Prozess zur Verwaltung eingehender Benachrichtigungen und Warnmeldungen
- [x] Dokumentationsmanagement
- [x] Richtlinien zum Gebrauch von Mobile Devices (z.B. ByoD)
- [x] Effektives Management zur Verhinderung von Schatten-IT, also dem Einsatz von IT-Systemen außerhalb der offiziellen IT-Infrastruktur
- [ ] Sonstige [bitte eintragen]

2. PHYSISCHE SICHERHEITSMASSNAHMEN

Der Auftragsverarbeiter muss Maßnahmen zur Gewährleistung der physischen Sicherheit, z.B. von Gebäuden und Hardware, ergreifen. Um Redundanzen zu vermeiden, sind im Folgenden nur Maßnahmen aufgelistet, die zu den oben genannten hinzukommen.

Die folgenden Maßnahmen sind beim Auftragsverarbeiter umgesetzt:

- [x] Ausreichende strukturelle Schutzmaßnahmen, die ein hohes Maß an Zuverlässigkeit und Sicherheit gegenüber Angriffen sowie Umweltbedrohungen gewährleisten (z. B. Standort und Konzeption des Rechenzentrums, keine Abhängigkeit vom Stromversorger)
- [x] Physikalische Redundanzen bezüglich zentraler Infrastrukturkomponenten (z. B. Netzzugang, Stromversorgung)
- [x] Angemessener Schutz der Räumlichkeiten vor physischem Eindringen durch sichere Zugangsbeschränkungsmechanismen (physische Zugangskontrolle)
  - [x] Türsicherheit (z. B. Verriegelung, elektrischer Öffner, Chipkarte / Magnet-karte, ID-Kartenleser)
  - [x] Überwachung und Montoring von Einrichtungsgegenständen und Assets (z. B. Alarmsystem, Videoüberwachung)
  - [ ] Sicherheitszonen mit unterschiedlichem Schutzniveau
  - [ ] Protokollierung physischer Zugriffsereignisse
  - [ ] Grundstücks- und Gebäudesicherheit (z. B. Pförtner)
  - [ ] Allgemeine Bestimmungen für den Zugang von externen Parteien
  - [ ] Isolierung sicherheitskritischer IT-Systeme (z. B. Drehkreuz, Sicherheitsverriegelungskorridor)
- [x] Vorschriften zur Nutzung / Entsorgung von Datenträgern (z. B. USB-Sticks, Mobiltelefone, externe Festplatten)
- [ ] Sonstige [bitte eintragen]

3. MASSNAHMEN ZUR SYSTEMSICHERUNG

Der Auftragsverarbeiter muss Maßnahmen ergreifen, um unter anderem Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit und Widerstandsfähigkeit des IT-Systems und der erbrachten Dienstleistungen zu gewährleisten. Um Redundanzen zu vermeiden, sind im Folgenden nur Maßnahmen aufgelistet, die zu den oben genannten hinzukommen.

Die folgenden Maßnahmen sind beim Auftragsverarbeiter umgesetzt:

- [x] Differenzierte Berechtigungskonzepte
  - [x] Rollenbasierte Zugriffskonzepte
  - [x] Umfassende Prüfung von Berechtigungen (analog zum Berechtigungskonzept)
  - [x] Sichere Identifizierungsmechanismen (für Benutzer und Administratoren)
  - [x] Anforderungen an die Authentifizierung:
    - [x] Individuelle IDs
    - [ ] Mindestanforderungen an das Passwort (z.B. Länge, Dauer, Zusammensetzung)
    - [ ] Multi-Faktor-Authentifizierung
    - [x] Automatisches Sperren nach einer bestimmten Anzahl von fehlgeschlagenen Anmeldeversuchen
    - [ ] Erforderliche Neuanmeldung nach einer bestimmten Zeit der Nichtbenutzung
  - [x] Weitere Zugriffsbeschränkungsmechanismen, um unbefugte Benutzung und Eindringen in das System zu verhindern (z.B. VPN)
  - [x] Verfahren für den schnellen Widerruf/ die Änderung von individuellen Rechten
- [ ] Monitoring:
  - [ ] Login-Versuche
  - [ ] Einführung eines Benutzerstammsatzes (enthält z.B. die Zuordnung einer oder mehrerer Rollen zu einem Benutzer)
  - [ ] Sichere und revisionssichere Aufbewahrung von Aufzeichnungen (z.B. sollte es für eine Person technisch unmöglich sein, die Ausführung einer früheren Aktion wirksam zu bestreiten)
- [x] Schutz vor Malware und Hacking:
  - [x] Anti-Viren-Software
  - [x] Firewalls
  - [x] Einsatz von Intrusion-Detection-Systemen
  - [ ] Implementierung eines Schwachstellenmanagementprozesses
  - [ ] Etablierung von Vermeidungsstrategien und -mechanismen (z.B. regelmäßige Analyse und Monitoring der Dokumentation)
  - [x] Sicherung von Schnittstellen (Benutzer/ Management)
  - [ ] Sichere Kommunikation (z.B. Verschlüsselung)
- [x] Isolation:
  - [x] Trennung verschiedener virtueller Maschinen (z.B. Hypervisoren)
  - [x] Trennung verschiedener Umgebungen (Entwicklung, Test, Produktion)
  - [ ] Trennung Verwaltungs- und Administrationsnetzwerk
- [x] Systemstabilität:
  - [x] Sicherstellung einer hohen Skalierbarkeit der Dienste
  - [x] Vereinfachung durch Virtualisierung, Standardisierung und Automatisierung
  - [ ] Leistungssteigerung (z.B. Verschlankung der Log-Mechanismen)
  - [x] Load-Balancing für dynamischen Lastausgleich (z.B. Pooling)
- [ ] Sonstige [bitte eintragen]

4. MASSNAHMEN ZUR DATENSICHERHEIT

Der Auftragsverarbeiter muss Maßnahmen zur Gewährleistung der Datensicherheit ergreifen. Dies schließt Maßnahmen ein, um die Verfügbarkeit und den Zugriff auf personenbezogene Daten im Falle eines physischen oder technischen Zwischenfalls zeitnah wiederherzustellen. Um Redundanzen zu vermeiden, sind im Folgenden nur Maßnahmen aufgelistet, die zu den oben genannten hinzukommen.

Die folgenden Maßnahmen sind beim Auftragsverarbeiter umgesetzt:

- [x] Sicherstellung der Integrität
  - [x] Maßnahmen zur Vermeidung unerwünschter Änderungen oder Löschungen von Daten
  - [ ] Systeme zur Überprüfung der Datenplausibilität
  - [ ] Lückenlose Protokollierung von Dateizugriffen und Änderungen
  - [ ] Absicherung des Managements von Systemlogs, Aufzeichnungen und Dokumentationen
  - [ ] Sonstige [bitte eintragen]

- [x] Sicherstellung der Vertraulichkeit:
  - [ ] Prozesse für Anonymisierung und Pseudonymisierung sind im Einsatz:
    [bitte eintragen, welche Daten im Verarbeitungsprozess an welcher Stelle anonymisiert werden]
    [bitte eintragen, welche Daten im Verarbeitungsprozess an welcher Stelle pseudonymisiert werden]

  - [x] Datenzugriffskontrollmaßnahmen:
  - [x] Verschlüsselung
    - [x] Angemessener Level der Verschlüsselung
    - [ ] Sichere Speicherung von Verwaltung von Schlüsseln
    - [ ] Regelmäßiger Wechsel der Schlüssel
    - [ ] Verfahren für den verlustfreien Widerruf von Schlüsseln

  - [x] Sichere Datenverarbeitung (während des gesamten Lebenszyklus):
  - [ ] Datensatztrennung zur Vermeidung von Kombination und unberechtigtem Zugriff (Hinweis: Selbst anonymisierte und pseudonymisierte Daten können zu persönlichen Daten werden, wenn sie mit anderen Informationen kombiniert werden)
  - [ ] Sicherstellung einer gesetzeskonformen und zeitnahen Datenlöschung (z.B. durch Überschreiben der Daten)
  - [ ] Sonstige [bitte eintragen]

- [x] Sicherstellung der Verfügbarkeit:
  - [x] Virtuelle Redundanzen (z.B. regelmäßige Daten-Backups) und Versionierung
  - [ ] Die Backups enthalten Installationen (z.B. Bare-Metal-Recovery), System- und Protokolldateien sowie Benutzerkonten und Konfigurationseinstellungen
  - [ ] Maßnahmen sind ergriffen, um die Verfügbarkeit und den Zugriff auf personenbezogene Daten im Falle eines physischen oder technischen Zwischenfalls zeitnah wiederherzustellen
  - [ ] Die Portabilität der personenbezogenen Daten ist durch Standardisierung und Bereitstellung entsprechender Schnittstellen sichergestellt
  - [ ] Sonstige [bitte eintragen]

- [ ] Sonstige [bitte eintragen]

5. PERSONAL

Der Bearbeiter führt regelmäßige Schulungen und Sicherheitsüberprüfungen in Bezug auf das Personal durch, einschließlich Schulungen zu den erforderlichen technischen und organisatorischen Maßnahmen. Um Redundanzen zu vermeiden, sind im Folgenden nur Maßnahmen aufgelistet, die zu den oben genannten hinzukommen.

Die folgenden Maßnahmen sind beim Auftragsverarbeiter umgesetzt:

- [x] Ernennung eines qualifizierten Datenschutzbeauftragten, sofern dies gesetzlich vorgeschrieben ist
- [ ] Definierte Verantwortlichkeiten und Vertretungsregelungen
- [x] Benutzerrichtlinien:
  - [x] Zur Schaffung eines Sicherheitsbewusstseins
  - [x] Verpflichtung des Personals auf Geheimhaltung
  - [ ] Sonstige [bitte eintragen]
- [x] Einstellung:
  - [ ] Sicherheitsüberprüfungen vor Einstellung
  - [ ] Maßnahmen zur Sicherstellung der Qualifikation
  - [x] Angemessene Einführungsschulungen
- [ ] Schulungen:
  - [ ] Regelmäßige Schulungen zu Systemsicherheit und Datensicherheit, um z.B. Risikobewusstsein schaffen
  - [ ] Laufende Trainings und Qualifizierungen
- [ ] Widerrufsverfahren zu priviligierten Rechten
- [ ] Mitarbeiter Feedback-Kanäle
- [ ] Sonstige [bitte eintragen]

6. BEWERTUNG

Der Auftragsverarbeiter muss ein Umfeld für die regelmäßige Überprüfung, Be-wertung und Kontrolle der Wirksamkeit technischer und organisatorischer Maß-nahmen zur Gewährleistung der Sicherheit der Verarbeitung gewährleisten. Um Redundanzen zu vermeiden, sind im Folgenden nur Maßnahmen aufgelistet, die zu den oben genannten hinzukommen.

Die folgenden Maßnahmen sind beim Auftragsverarbeiter umgesetzt:
☐ Implementierung eines Prozesses zur regelmäßigen Überprüfung, Beurteilung und Bewertung der Wirksamkeit von technischen und organisatorischen Maß-nahmen zur Gewährleistung der Sicherheit der Verarbeitung
☒ Regelmäßige Durchführung und Dokumentation von Datenwiederherstellungstests
☐ Regelmäßige Prüfungen durch unabhängige Datenschutzexperten
☐ Penetrationstests
☐ Sonstige [bitte eintragen]

7. ZERTIFIKATE

Der Auftragsverarbeiter besitzt folgende Zertifikate:

ANLAGE 3: UNTERBEAUFTRAGUNGEN

Gemäß Abschnitt 2.9.1 stimmt der Controller der Untervergabe von Verarbeitungsaktivitäten durch den Auftragsverarbeiter an folgende Subunternehmer zu:

Lfd.Nr.	Unterbeauftragter	Anschrift	Zweck der Unterbeauftragung
1	Diverse Spediteure		Auslieferung von Produkten im Rahmen der Partnervereinbarung
2	Limex Computer GmbH	Holsten-Mündruper-Straße 80 49086 Osnabrück Deutschland	Annahme von Bestellungen von Benutzern der WM Kataloge und Betrieb der RepDoc-Cloud-Plattform
3	DVSE Gesellschaft für Datenverarbeitung, Service & Entwicklung mbH	Lise-Meitner-Straße 4 22941 Bargteheide Deutschland	Annahme von Bestellungen von Benutzern der WM Kataloge
4	Robert Bosch GmbH	Wernerstraße 51 70469 Stuttgart Deutschland	Kundenberatung für Nutzer der technischen Hotline von Bosch
5	Asanetwork GmbH	Vennhauser Allee 265 40627 Düsseldorf Deutschland	Für die Verknüpfung anderer Software in der Werkstatt mit den Diagnosegeräten
6	Hella Gutmann Solutions A/S	Lundborgvej 10 8800 Viborg Dänemark	Für die korrekte Fahrzeugaus-wahl
7	TecAlliance GmbH	Steinheilstraße 10 85737 Ismaning Deutschland	Für die korrekte Identifikation von Fahrzeugen in Österreich, Schweiz, Deutschland, Frankreich und Niederlande
8	Bisnode Danmark a/s	Gyngemose Parkvej 50, 8 2860 Søborg Dänemark	Für die korrekte Identifikation von Fahrzeugen in Finnland, Norwegen und Schweden
9	FTZ Autodele & Værktøj A/S	Hvidkærvej 21 5250 Odense SV Dänemark	Für die korrekte Identifikation von Fahrzeugen in Dänemark
10	Jifeline BV	De Hoogjens 11 4254 XV Sleeuwijk Niederlande	Für die Durchführung von Diagnose-/ Codier-Dienstleistungen über das Internet
11	APIZEE	11 street Blaise Pascal 22300 Lannion Frankreich	Für die Durchführung von Remote Support Sessions per Video/Audio/Chat

Lfd.Nr.	Unterbeauftragter	Anschrift	Zweck der Unterbeauftragung
12	AWS	Amazon Web Services Inc. 410 Terry Avenue North, Seattle, WA 98109-5210, USA	Für die Bereitstellung von Onlinedienstleistungen
13	TecMotive GmbH	Wilmersdorfer Str. 115-116 10627 Berlin Deutschland	Für die Durchführung von Servicedienstleistungen
14	IDnow GmbH	Auenstr. 100 80469 München Deutschland	Identitätsprüfung/Verifikation des Mitarbeiters in der Werkstatt
15	FCA Italy S.p.A.	C.so G. Agnelli 200 10135 Turin Italien	Authentifizierter Diagnosezugriff (Security Gateway)
16	Mercedes-Benz AG	Mercedesstraße 120 70372 Stuttgart Deutschland	Zertifikatbasirte Diagnose (CeBAS)
17	VOLKSWAGEN AG	Berliner Ring 2 38440 Wolfsburg Deutschland	Schutz der Fahrzeugdiagnose (SFD)
18	WM SE	Pagenstecherstraße 121 49090 Osnabrück Deutschland	Datenübermittlung zur Berechnung für Remote-Dienstleistung an WM-Kunden