Stand: Februar 2025

Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DS-GVO

zwischen dem

Kunden

- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

Wacker Neuson SE

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Auftragnehmer verarbeitet die in Ziffer 2 (2) genannten Daten im Rahmen der Erbringung von Telematikdiensten für den Kunden (im Folgenden „**Personenbezogene Kundendaten**“). Der Gegenstand des Auftrags ergibt sich aus dem Antrag des Kunden auf einen Wacker Neuson Group EquipCare Account, in den auch diese Vereinbarung zur Auftragsverarbeitung (diese „**Vereinbarung**“) einbezogen wird, in Verbindung mit den dort ebenfalls einbezogenen Allgemeinen EquipCare Geschäftsbedingungen (im Folgenden „**Leistungsvereinbarung**“).

(2) Dauer

Der Auftrag dauert solange wie die Leistungsvereinbarung fortbesteht. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Sofern die Erbringung der Verarbeitungsleistungen, die Gegenstand dieser Vereinbarung sind, nach Beendigung der Leistungsvereinbarung noch nicht abgeschlossen ist, oder der Auftragnehmer sonst nach Beendigung der Leistungsvereinbarung oder Kündigung dieser Vereinbarung noch Personenbezogene Kundendaten verarbeitet, endet die Laufzeit dieser Vereinbarung erst mit dem Abschluss der Erbringung der Verarbeitungsleistungen und der vollständigen Löschung oder Rückgabe der Personenbezogenen Kundendaten an den Auftraggeber.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Personenbezogenen Kundendaten

Art und Zweck der Verarbeitung Personenbezogener Kundendaten durch den Auftragnehmer für den Auftraggeber beinhaltet Rohdaten- sowie Backend- bzw. Frontend-Verarbeitung der Maschinen- und Geolokalisationsdaten zu Zwecken des Flottenmanagement, der Einsatzplanung und Standorterkennung für Serviceleistungen. Die Verarbeitung schließt Personenbezogene Kundendaten ein, zu Zwecken des Lizenzmanagements, der Identifikation, Authentisierung und Autorisierung natürlicher Personen bei der Nutzung der Telematikdienste. Die Übermittlung der Geolokationsdaten erfolgt über alle technisch verfügbaren Möglichkeiten, wie beispielsweise GPS und Bluetooth. Die

Maschinendaten umfassen, je nach Gerätetyp unter anderem Betriebsstunden, gefahrene Kilometer, Akkuspannung, Seriennummer, Fehlerdiagnose. Des Weiteren können diese Maschinendaten, auf Antrag des Auftraggebers, verarbeitet werden um Handlungsempfehlungen im Maschinenumgang, wie beispielsweise Motoranpassungen aufgrund von topographischen Extremsituationen bereitstellen zu können.

Anlage 2 enthält detaillierte Weisungen des Auftraggebers in Bezug auf die Übermittlung Personenbezogener Kundendaten an

Dritte. Außerdem anonymisiert der Auftragnehmer Personenbezogene Kundendaten, die Gegenstand dieser Vereinbarung sind im Auftrag des Auftraggebers. Anonymisierte Daten sind keine Personenbezogenen Kundendaten im Sinne dieser Vereinbarung. Der Auftragnehmer ist berechtigt, diese anonymisierten Daten auch für eigene Zwecke zu nutzen.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet statt (i) in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum und/oder (ii) in den in Anlage 3 bzw. in der jeweiligen Anzeige zur Beauftragung eines weiteren Unterauftragnehmers oder des Wechsels eines bestehenden Unterauftragnehmers nach Ziffer 6 identifizierten Drittländern, wenn hierfür die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

(2) Art der Daten

Gegenstand der Verarbeitung Personenbezogener Kundendaten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

☒ Kundenstammdaten (soweit der Auftragnehmer diese nicht als Verantwortlicher nutzt)

☒ Logindaten (E-Mail, Passwort)

☒ Planungs- und Steuerungsdaten

☒ Geolokalisationsdaten

☒ Maschinendaten

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

☒ Beschäftigte des Auftraggebers und i. S. d. AktG verbundener Unternehmen
☐ Beschäftigte des Auftragnehmers und i. S. d. AktG verbundener Unternehmen
☐ Beschäftigte von Vertriebspartnern des Auftragnehmers

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren.

(2) Der Auftragnehmer hat bezogen auf seine Verarbeitungsprozesse im Rahmen dieses Auftrags die Sicherheit gemäß Art. 28 Abs. 3 lit. c, 32 DS-GVO, insbesondere in Verbindung mit Art. 5 Abs. 1,

Abs. 2 DS-GVO, 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 DS-GVO zu berücksichtigen. Konkret trifft der Auftragnehmer die in **Anlage 1** niedergelegten Maßnahmen.

(3) 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 zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Personenbezogenen Kundendaten

Der Auftragnehmer darf Personenbezogene Kundendaten nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich oder wegen der Geltendmachung anderer Betroffenenrechte unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu Personenbezogenen Kundendaten hat, dürfen diese Daten ausschließlich entsprechend der dokumentierten Weisung des Auftraggebers verarbeiten, es sei denn, dass sie nach dem Recht der EU oder eines Mitgliedstaats der EU zur Verarbeitung entgegen dieser Weisungen verpflichtet sind. 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.
c) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
d) 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 Kundendaten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
e) 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 auf Anfrage angemessen zu unterstützen.
f) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem

Verantwortungsbereich als Auftragsverarbeiter im Einklang mit den Anforderungen des Art. 28 DS-GVO erfolgt.

g) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieser Vereinbarung.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die „weitere Auftragsverarbeiter" im Sinne des Art. 28 (4) DS-GVO für den Auftragnehmer im Namen des Verantwortlichen erbringen.Der Auftraggeber stimmt der Beauftragung der in **Anlage 3** aufgeführten Unterauftragnehmer zu, unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 4 DS-GVO.

(2) Für die Beauftragung weiterer Unterauftragnehmer oder den Wechsel eines bestehenden Unterauftragnehmers erteilt der Auftraggeber hiermit seine allgemeine Genehmigung im Sinne des Art. 28 Abs. 2 DS-GVO. Eine solche Beauftragung bzw. ein solcher Wechsel sind zulässig, soweit:

- der Auftragnehmer eine solche Beauftragung dem Auftraggeber mit angemessenem zeitlichem Vorlauf vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht gegenüber dem Auftragnehmer schriftlich oder in Textform wirksam Einspruch gegen die geplante Beauftragung erhebt;
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 4 DS-GVO zugrunde gelegt wird.

Ein Einspruch des Auftraggebers gegen eine beabsichtigte Änderung in Bezug auf die Beauftragung eines weiteren Unterauftragnehmers oder den Wechsel eines bestehenden Unterauftragnehmers ist nur wirksam, wenn er aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erfolgt. Ein wichtiger Grund liegt nur vor, wenn die Änderung dem Auftraggeber unter Berücksichtigung aller Umstände und unter Abwägung der beiderseitigen Interessen unzumutbar ist. Der Einspruch ist überdies nur wirksam, wenn er innerhalb der in der Anzeige des Auftragnehmers angegebenen Frist beim Auftragnehmer zugeht. Diese Frist muss mindestens zwei (2) Wochen ab Zugang der Anzeige des Auftragnehmers beim Auftraggeber betragen.

Im Falle eines Einspruchs kann der Auftragnehmer die Leistungsvereinbarung einschließlich dieser Vereinbarung zur Auftragsverarbeitung mit Wirkung zu dem Zeitpunkt kündigen, an dem der Auftragnehmer die Beauftragung eines weiteren Unterauftragnehmers oder den Wechsel eines bestehenden Unterauftragnehmers beginnen und diesem Unterauftragnehmer Zugriff auf Personenbezogene Kundendaten gewähren möchte. Diesen Zeitpunkt weist der Auftragnehmer in der Anzeige der geplanten Beauftragung eines weiteren Unterauftragnehmers oder des Wechsels eines bestehenden Unterauftragnehmers aus.

(3) Die Weitergabe Personenbezogener Kundendaten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher und informiert den Auftraggeber hierüber in Anlage 3 bzw. in der jeweiligen Anzeige zur Beauftragung eines weiteren Unterauftragnehmers oder des Wechsels eines bestehenden Unterauftragnehmers. Soweit zur Herstellung der datenschutzrechtlichen Zulässigkeit solcher Übermittlungen außerhalb der EU/des EWR die Mitwirkung des Auftraggebers erforderlich ist, unterstützt der Auftraggeber den Auftragnehmer im erforderlichen Maß auf Anfrage.

7. Kontrollrechte des Auftraggebers

(1) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber nach Maßgabe der Absätze (2) und (3) von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO 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.

(2) Der Nachweis solcher Maßnahmen, die den Auftrag betreffen, kann nach billigem Ermessen des Auftragnehmers insbesondere erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI Grundschutz).

(3) Der Auftraggeber hat außerdem das Recht, Überprüfungen – einschließlich Inspektionen – selbst durchzuführen oder durch einen von ihm beauftragten Prüfer durchführen zu lassen. Der Auftragnehmer wird solche Überprüfungen ermöglichen und dazu beitragen.

(4) Der Auftraggeber informiert den Auftragnehmer rechtzeitig, im Regelfall mindestens zwei (2) Wochen im Voraus, über die Durchführung einer Überprüfung, einschließlich einer Inspektion. In dringenden, vom Auftraggeber nachzuweisenden und zu begründenden Ausnahmefällen ist der Auftraggeber berechtigt, eine Überprüfung, einschließlich einer Inspektion, ohne Vorankündigung durchzuführen, wenn anderenfalls der Kontrollzweck gefährdet wäre.

(5) Der Auftraggeber führt Inspektionen in der Regel während der normalen Geschäftszeiten des Auftragnehmers durch.

(6) Der Zutritt zu den Räumlichkeiten des Auftragnehmers erfolgt ausschließlich im ständigen Beisein eines Vertreters des Auftragnehmers. Diesem Vertreter obliegt die Entscheidungsbefugnis über den Ablauf der Kontrolle insoweit, wie dies erforderlich ist, um übermäßige Störungen des Betriebsablaufs des Auftragnehmers zu verhindern und Geheimhaltungspflichten des Auftragnehmers gegenüber Dritten zu wahren.

(7) Betriebs- und Geschäftsgeheimnisse des Auftragnehmers, die dem Auftraggeber im Zuge einer solchen Kontrolle bekannt werden, sind vom Auftraggeber streng vertraulich zu behandeln. Aufzeichnungen hierüber dürfen nicht stattfinden, soweit dies nicht zwingend für die Ausübung des Kontrollrechts des Auftraggebers erforderlich ist.

(8) Reguläre Kontrollen vor Ort seitens des Auftraggebers nach Maßgabe von Absatz (3) sind in der Regel maximal einmal pro Kalenderjahr zulässig. Zusätzliche Kontrollen durch den Auftraggeber nach Maßgabe von Absatz (3) können nur aus wichtigem, vom Auftraggeber nachzuweisenden Grund durchgeführt werden.

(9) Für die Ermöglichung von Kontrollen durch den Auftraggeber und zur Unterstützung des Auftraggebers bei diesen Kontrollen kann der Auftragnehmer die Erstattung ihm hierdurch entstehender, angemessener Aufwände verlangen, es sei denn, etwaige bei der Kontrolle festgestellte Mängel beruhen auf einem schuldhaften Verstoß des Auftragnehmers gegen diese Vereinbarung, Weisungen des Auftraggebers oder für den Auftragnehmer anwendbare Gesetze.

8. Unterstützungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit Personenbezogener Kundendaten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u. a.

a) 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
b) die Verpflichtung, Verletzungen der Verfügbarkeit, Vertraulichkeit oder Integrität Personenbezogener Kundendaten im Sinne des Art. 33 DS-GVO unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Der Auftragnehmer wird den Auftraggeber - nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen - im Rahmen des Zumutbaren und Erforderlichen unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Person in Bezug auf ihre Personenbezogenen Kundendaten nachzukommen, soweit solche Anträge die von dieser Vereinbarung erfassten Personenbezogenen Kundendaten betreffen, insbesondere hinsichtlich deren Rechte aus Art. 12 bis 23 DS-GVO.

(3) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) 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 solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe Personenbezogener Kundendaten

(1) Kopien oder Duplikate Personenbezogener Kundendaten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Während der Laufzeit der Leistungsvereinbarung und für bis zu 10 Tage nach deren Beendigung ermöglicht der Auftragnehmer es dem Auftraggeber, dass der Auftragnehmer dem Auftraggeber nach in Textform erklärter Anforderung des Auftragnehmers seine Personenbezogenen Kundendaten in einem maschinenlesbaren Format übermittelt oder diese löscht. Nach Ablauf dieser Frist wird der Auftraggeber, vorbehaltlich der Absätze (3) und (4), sämtliche in den Diensten

vorhandenen Personenbezogenen Kundendaten des Auftraggebers löschen und etwaige sonstige in seinen Besitz gelangten Personenbezogenen Kundendaten, die der Auftragnehmer unter dieser Vereinbarung vom Auftraggeber erhalten hat, dem Auftraggeber aushändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial.

(3) Die vorgenannten Löschpflichten gelten nicht

(i) für Kopien von Personenbezogenen Kundendaten, die auf Backup-Medien und/oder Backup Servern gespeichert sind, bis deren Löschung gemäß anerkannten Prozeduren der Informationssicherheit vorgesehen ist, wobei der Auftragnehmer vorbehaltlich der lit. (ii) solche aufbewahrten Daten und Unterlagen für keine anderen als Backup-Zwecke nutzen wird und die Bestimmungen dieser Vereinbarung bezogen auf diese temporäre Speicherung weiterhin Anwendung finden;

(ii) soweit der Auftragnehmer nach dem Recht der EU oder eines Mitgliedstaats der EU zur Speicherung der Personenbezogenen Kundendaten verpflichtet ist.

(4) Einer Vernichtung oder Löschung Personenbezogener Kundendaten steht die Anonymisierung dieser Daten durch den Auftragnehmer gleich.

(5) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Ende dieser Vereinbarung hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Ende dieser Vereinbarung dem Auftraggeber übergeben.

11. Freistellung

(1) Sollten Dritte, insbesondere betroffene Personen, gegen den Auftragnehmer aufgrund oder im Zusammengang mit der Verarbeitung Personenbezogener Kundendaten, die Gegenstand dieser Vereinbarung sind, Ansprüche gegen den Auftragnehmer geltend machen („Ansprüche Dritter“), kann der Auftragnehmer verlangen, dass der Auftraggeber die Abwehr der Ansprüche Dritter übernimmt und den Auftragnehmer von den Ansprüchen Dritter freistellt, soweit sie durch rechtskräftiges Urteil festgestellt oder mit Zustimmung des Auftragnehmers vom Auftraggeber verglichen oder anerkannt werden. Der Auftraggeber hat die Kosten im Zusammenhang mit der Abwehr bzw. vergleichsweisen Regelung der Ansprüche Dritter zu tragen und dem Auftragnehmer derartige ggf. bei ihm anfallende Kosten zu erstatten. Gleiches gilt für jegliche Kosten, die dem Auftragnehmer durch etwaige Maßnahmen von Aufsichtsbehörden aufgrund der Verarbeitung Personenbezogener Kundendaten im Rahmen dieser Vereinbarung und der Weisungen des Auftraggebers entstehen.

(2) Verlangt der Auftragnehmer vom Auftraggeber ein Vorgehen gemäß Absatz (1), wird der Auftragnehmer dem Auftraggeber im Innenverhältnis die alleinige Kontrolle über die Abwehr der Ansprüche Dritter überlassen und den Auftraggeber im Rahmen des Zumutbaren bei der Abwehr dieser Ansprüche Dritter auf Kosten des Auftraggebers unterstützen.

(3) Der Auftraggeber ist nicht zur Freistellung nach Absatz (1) verpflichtet, soweit die Ansprüche Dritter (i) aus einer Verletzung dieser Vereinbarung durch den Auftragnehmer oder (ii) speziell aus einer Anonymisierung der Personenbezogenen Kundendaten und der Nutzung dieser anonymisierten Daten für Zwecke des Auftragnehmers resultieren.

12. Anlagen

Anlage 1: Technisch-Organisatorische Maßnahmen

Anlage 2: Spezifische Weisungen des Auftraggebers zur Übermittlung Personenbezogener Kundendaten an Dritte

Anlage 3: Unterauftragnehmer

Anlage 1

Technische und organisatorische Maßnahmen

Für die Darstellung der grundlegenden technischen und organisatorischen Maßnahmen der Unterauftragnehmerdienste Microsoft Azure und Amazon Web Service, einschließlich der Maßnahmen zur Gebäudesicherheit, sowie einschlägige Zertifizierungen konsultieren Sie bitte:

Microsoft Azure: https://docs.microsoft.com/de-de/azure/security/

Amazon Web Services: https://aws.amazon.com/de/security/

Darüber hinaus wurden die folgenden wesentlichen technischen und organisatorischen Maßnahmen implementiert, um die Sicherheit der Verarbeitung personenbezogener Kundendaten in EquipCare gemäß Art. 32 DSGVO umfassend sicherzustellen:

(1) Pseudonymisierung Personenbezogener Kundendaten (Artikel 32 (1) (a) DS-GVO)

- Trennung der Verarbeitungswege in der Backend-Verarbeitung mit und ohne personenbezogene Daten (vollständige Anonymisierung).

(2) Verschlüsselung Personenbezogener Kundendaten (Artikel 32 (1) (a) DS-GVO)

- Transportverschlüsselung nach Stand der Technik, vornehmlich bei Netzwerkprotokollen und Schnittstellen (bspw. API).
- Lagerverschlüsselung in Backend-Verarbeitung für personenbezogene Daten, vornehmlich im Rahmen des Identitätsmanagements.

(3) Fähigkeit, die Vertraulichkeit von Verarbeitungssystemen und -diensten auf Dauer sicherzustellen (Artikel 32 (1) (b) DS-GVO)

- Mitarbeiter mit autorisiertem Zugang zu personenbezogene Kundendaten sind zur Vertraulichkeit verpflichtet und regelmäßig geschult.
- Einsatz eines mehrstufigen, aktuellen Anti-Malware-Systems.
- Zugriffskontrollen und Rollenkonzept auf Basis der Prinzipien "Least Privilege", "Need-to-know" und "Segregation of Duty".
- Trennung von technischem und inhaltlichem Betrieb der Telematiklösung.
- Physische Zugangsbeschränkungen zu Server- und Kommunikationsräumen.
- Externe werden registriert, in einem Protokoll erfasst und dauerhaft begleitet

(4) Fähigkeit, die Integrität von Verarbeitungssystemen und -diensten auf Dauer sicherzustellen (Artikel 32 (1) (b) DS-GVO)

- Protokollierung aller Zugriffe, Änderungen und Löschungen mit individuellen Benutzernamen.
- Rollenkonzept zur Steuerung von Berechtigungen (bspw. Lesen, Schreiben, Verwalten von Daten).
- Einsatz von VPN-Verbindungen und E-Mail-Transportverschlüsselung.
- Verschlüsselung und Authentizitätsprüfung der Firmware in den Telematikmodulen.

(5) Fähigkeit, die Verfügbarkeit von Verarbeitungssystemen und -diensten auf Dauer sicherzustellen (Artikel 32 (1) (b) DS-GVO)

- Implementierung eines üblichen Backup- und Wiederherstellungskonzepts, um den Verlust von Daten zu verhindern.
- Mehrstufiges Antiviren- und Firewall-Konzept mit regelmäßigen Aktualisierungen.
- 24/7 Monitoring kritischer Dienste.
- Regelmäßige Tests zur Überprüfung der Datenwiederherstellung und Dokumentation der Ergebnisse.

(6) Fähigkeit, die Belastbarkeit von Verarbeitungssystemen und -diensten auf Dauer sicherzustellen (Artikel 32 (1) (b) DS-GVO)

- Implementierung von Prozessen zur kontinuierlichen Überwachung, Erkennung und Reaktion auf Sicherheitsschwachstellen.
- Regelmäßige Überprüfung von Schwachstellen-Warnungen und Durchführung von Penetrationstests.

(7) Fähigkeit, die Verfügbarkeit der Personenbezogenen Kundendaten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Artikel 32 (1) (c) DS-GVO)

- Regelmäßige Tests zur Überprüfung der Datenwiederherstellung und Dokumentation der Ergebnisse.
- Sichere Aufbewahrung von Sicherungsmedien in getrennten Brandabschnitten.
- Implementierung eines Intrusion-Detection-Systems (IDS).
- Erstellung und Pflege von Notfall- und Alternativplänen.
- 24/7 Monitoring kritischer Dienste.

(8) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Artikel 32 (1) (d) DS-GVO)

- Regelmäßige Prüfungen der Sicherheit der Verarbeitungsumgebung.
- Regelmäßige Überprüfung der Konzeptions- und Dokumentationsbasis.
- Regelmäßige Schulungen für Mitarbeiter mit autorisiertem Zugriff auf personenbezogene Kundendaten.
- Zentrale Dokumentation aller Datenschutzverfahren und -regelungen mit Zugriffsmöglichkeit für Mitarbeiter.
- Einbettung der Verarbeitungstätigkeit in die Security, Risikomanagement- und Business Continuity Rahmenwerke mit kontinuierlichem Verbesserungsprozess.
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen.

Anlage 2

Spezifische Weisungen des Auftraggebers zur Übermittlung Personenbezogener Kundendaten an Dritte

Nach der Leistungsvereinbarung ermöglicht die Telematiklösung den Zugriff auf Personenbezogene Kundendaten durch den Auftragnehmer, andere Unternehmen der Wacker Neuson Group sowie durch Vertriebspartner des Auftragnehmers jeweils zu eigenen Geschäftszwecken (etwa Erbringung von EquipCare Services auf Anfrage des Auftraggebers oder zur Produktentwicklung).

Konkret sollen folgende Empfänger Zugriff auf Personenbezogene Kundendaten für deren folgende eigene Geschäftszwecke erhalten:

Empfänger	**Jeweiliger eigener Geschäftszweck**
Wacker Neuson SE	• Second Level Support (auf konkrete Supportanfrage des Auftraggebers)
Produktionsgesellschaft (der Wacker Neuson Gruppe), die die jeweilige Maschine produziert hat, aus der die jeweiligen Personenbezogenen Kundendaten übermittelt wurden.	• Second Level Support (auf konkrete Supportanfrage des Auftraggebers) • Produktentwicklung • Prüfung etwaiger Gewährleistungs- oder Garantieansprüche
Vertriebsgesellschaft (der Wacker Neuson Gruppe), die die jeweilige Maschine, aus der die jeweiligen Personenbezogenen Kundendaten übermittelt wurden, direkt an den Auftraggeber, einen etwaigen Vorbesitzer oder sonst als Zwischenhändler verkauft hat.	• First Level Support (auf konkrete Supportanfrage des Auftraggebers) • Prüfung etwaiger Gewährleistungs- oder Garantieansprüche
Händler (Vertriebspartner), der die jeweilige Maschine, aus der die jeweiligen Personenbezogenen Kundendaten übermittelt wurden, an den Auftraggeber oder einen etwaigen Vorbesitzer verkauft hat.	• First Level Support (auf konkrete Supportanfrage des Auftraggebers) • Prüfung etwaiger Gewährleistungs- oder Garantieansprüche

Der Auftraggeber erteilt dem Auftragnehmer hiermit die Weisung, Personenbezogene Kundendaten im Wege der Einräumung von Zugriffsrechten an die oben genannten Empfänger zu den dort genannten Zwecken zu übermitteln, soweit dies für die jeweiligen oben genannten eigenen Geschäftszwecke dieser Empfänger erforderlich ist. Insoweit handeln diese Empfänger jeweils als Verantwortliche im Sinne des Art. 4 (7) DS-GVO.

Soweit der Auftragnehmer selbst Empfänger der jeweiligen Personenbezogenen Kundendaten ist, verpflichtet der Auftragnehmer sich hiermit gegenüber dem Auftraggeber, die Personenbezogenen Kundendaten ausschließlich für die oben genannten Zwecke zu verarbeiten und die Herstellung eines direkten Personenbezugs bestmöglich zu vermeiden. Der Auftragnehmer verpflichtet sich auch, keine Kopien Personenbezogener Kundendaten anzufertigen, sondern Personenbezogene Kundendaten ausschließlich in dem vom Auftragnehmer betriebenen Portal (gemäß Definition in der Leistungsvereinbarung) zu verarbeiten. Dies schränkt nicht die Erstellung von Kopien anonymisierter Informationen ein.

Anlage 3

Unterauftragnehmer

Rohdatenverarbeitung der Maschinen- und Geolokalisationsdaten			
Firma Unterauftragnehmer	Anschrift/Land	Leistung	Angaben zu geeigneten Garantien bei Datenübermittlungen in ein Drittland
Trackunit ApS	Gasværksvej 24, 9000 Aalborg, Dänemark	Rohdatenverarbeitung der Telematikdienste einschließlich Geolokalisationsdaten	
Trackunit ApS beauftragt entsprechende Unterunterauftragnehmer, die in folgender Quelle abrufbar sind: https://content.trackunit.com/hubfs/PDF%20Assets/Legal%20Documents/Trackunit%20%7C%20Policy%20%7C%20Sub%20Processor%20List%20%7C%202021-11%20%7C%20EN.pdf			Standardvertragsklauseln / SCC (EU)

Backend-Verarbeitung der Maschinen- und Geolokalisationsdaten einschließlich Personenbezogener Kundendaten			
Firma Unterauftragnehmer	Anschrift/Land	Leistung	Angaben zu geeigneten Garantien bei Datenübermittlungen in ein Drittland
Wacker Neuson Beteiligung GmbH	Flughafenstr. 7 4063 Hörsching, Österreich	Technischer Betrieb des Microsoft Azure Tenants und dessen Ressourcengruppen	
Wacker Neuson Produktion GmbH & Co. KG	Münchner Straße 31, 85084 Reichertshofen, Deutschland	Technischer Betrieb der zu den Telematikdiensten gehörenden Ressourcengruppen	
Wacker Neuson Aftermarket & Services GmbH	Preußenstraße 41, 80809 München, Deutschland	Lizenzmanagement für die Telematikdienste, Produktentwicklung und -betreuung der Telematikdienste sowie Marktanalysen	

Microsoft Ireland Operations, Ltd.	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland	Rohdatenverarbeitung der Telematikdienste einschließlich Geolokalisationsdaten, weitere Verarbeitung wie ordnen, speichern, visualisieren, übermitteln; Verarbeitung auf Servern in der Region Europa/West	
Microsoft beauftragt entsprechende Unterunterauftragnehmer, die in folgender Quelle abrufbar sind: https://servicetrust.microsoft.com/DocumentPage/badc200c-02ab-43d9-b092-ed9b93b9b4a8			Für die USA: Angemessenheitsbeschluss bzw. EU-U.S. Data Privacy Framework Für andere Drittländer: Standardvertragsklauseln / SCC (EU)
SAP SE	Dietmar-Hopp-Allee 16 69190 Walldorf Germany	Verarbeitung Personenbezogener Kundendaten zu Zwecken der Identifikation, Authentisierung und Autorisierung natürlicher Personen (Identitätsmanagement); Verarbeitung auf Servern in der Region Europa	
SAP SE beauftragt weitere Unterunterauftragnehmer. Die aktuelle Liste der Auftragnehmerschaften der SAP SE kann beim Auftragnehmer angefordert werden.			

Frontend-Datenverarbeitung			
Firma Unterauftragnehmer	Anschrift/Land	Leistung	Angaben zu geeigneten Garantien bei Datenübermittlungen in ein Drittland
OneStop Pro Software Solutions GmbH	Tittlinger Str. 39, DE-94034 Passau	Betrieb, Wartung und Entwicklung der Frontend-Telematikdienste	
OneStop Pro Software Solutions GmbH. beauftragt weitere Unterunterauftragnehmer. Die aktuelle Liste der Auftragnehmerschaften der OneStop Pro Software Solutions GmbH. kann beim Auftragnehmer angefordert werden.			