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 Verbindung mit den 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.

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 sind die Erbringung von Dienstleistungen im Zusammenhang mit Telematikdiensten, einschließlich Geolokalisation, Übermittlung und Auswertung von Maschinendaten, Predictive Maintenance und Handlungsempfehlungen im Maschinenumgang. **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 anonymen 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 einem Drittland, 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

(1) 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.

(2) Soweit vom standardmäßigen Umfang der Telematikdienste umfasst, unterstützt der Auftragnehmer den Auftraggeber bei dessen Erfüllung der Betroffenenrechte gemäß Ziffer 8 (2).

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.
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.

(2) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu, unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragnehmer	Land	Leistung

Amazon (AWS)	Irland, UK, Deutschland	Speicherung und Verarbeitung der Personenbezogenen Kundendaten „off site“
Zitcom A/S	Dänemark	Speicherung und Verarbeitung der Personenbezogenen Kundendaten „on site“
OKTA Inc.	Tenant Europa	Identity und Access Management
Trackunit A/S	Dänemark	Wartung und Entwicklung der Telematikdienste
Trackunit AB	Schweden	Wartung und Entwicklung der Telematikdienste
Trackunit AS	Norwegen	Wartung und Entwicklung der Telematikdienste
Trackunit B.V.	Niederlande	Wartung und Entwicklung der Telematikdienste
Trackunit GmbH	Deutschland	Wartung und Entwicklung der Telematikdienste
Trackunit Inc.	USA	Wartung und Entwicklung der Telematikdienste
Trackunit Ltd.	UK	Wartung und Entwicklung der Telematikdienste
Trackunit SAS	Frankreich	Wartung und Entwicklung der Telematikdienste

Die Beauftragung weiterer Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Beauftragung dem Auftraggeber mit angemessenem zeitlichem Vorlauf vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht innerhalb von 10 Werktagen nach dieser Anzeige gegenüber dem Auftragnehmer schriftlich oder in Textform wegen eines berechtigten Interesses aus Gründen des Datenschutzes Einspruch gegen die geplante Beauftragung erhebt;
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 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 aus wichtigem, dem Auftragnehmer nachzuweisenden Grund zulässig. Ein wichtiger Grund liegt nur vor, wenn die Änderung dem Auftraggeber unter Berücksichtigung aller Umstände und unter Abwägung der beiderseitigen Interessen unzumutbar ist. Der Auftraggeber kann nur innerhalb einer angemessenen Frist (in der Regel zwei (2) Wochen) Einspruch erheben, nachdem er vom Auftragnehmer über die Änderung informiert wurde.

Im Falle eines zulässigen 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. Der Auftraggeber erteilt dem Auftragnehmer hiermit die Berechtigung, im Namen des Auftraggebers EU-Standardvertragsklauseln (controller-to-processor) als „data exporter“ mit etwaigen Subunternehmern in Drittländern außerhalb des Europäischen Wirtschaftsraums zu schließen. Auf Anfrage des Auftraggebers legt der Auftragnehmer dem Auftraggeber die in dessen Namen abgeschlossenen EU-Standardvertragsklauseln vor.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

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 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) Ist der Auftraggeber der Ansicht, dass die in Absatz (2) beschriebenen Nachweise nicht ausreichen oder dass ein Verstoß gegen diese Vereinbarung oder die anwendbaren gesetzlichen Anforderungen vorliegt, hat der Auftraggeber das Recht, durch einen von ihm beauftragten unabhängigen und gesetzlich bzw. standesrechtlich zur Verschwiegenheit verpflichteten Dritten („Auditor“) im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer

durchführen zu lassen. Zu diesem Zweck hat der Auftraggeber das Recht, sich durch Stichprobenkontrollen – vorzunehmen durch den Auditor –, die rechtzeitig (in der Regel zwei (2) Wochen vor der geplanten Kontrolle) anzumelden sind, zu den üblichen Geschäftszeiten von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. 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 Störungen des Betriebsablaufs des Auftragnehmers zu verhindern und Geheimhaltungspflichten des Auftragnehmers gegenüber Dritten zu wahren.

(4) 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.

(5) Reguläre Kontrollen vor Ort seitens des Auftraggebers nach Maßgabe von Absatz (3) sind 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.

(6) 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 oder Weisungen des Auftraggebers.

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 diesem Vertrag zur Verarbeitung im Auftrag 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 dieses Vertrags bezogen auf diese temporäre Speicherung weiterhin Anwendung finden;

(ii) soweit der Auftragnehmer rechtlich 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 Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Freistellung

Sollten Dritte, insbesondere betroffene Personen, gegen den Auftragnehmer aufgrund oder im Zusammengang mit der Verarbeitung Personenbezogener Kundendaten, die Gegenstand dieses Vertrages 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 dieses Vertrages 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 dieses Vertrags 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 1

Technische und organisatorische Maßnahmen

Die folgenden Absätze beschreiben die technischen und organisatorischen Maßnahmen zur Gewährleistung der sicheren Verarbeitung personenbezogener Daten in EquipCare gemäß Art. 32 DSGVO. Soweit nicht anders angegeben, gelten die Maßnahmen gleichermaßen für den Auftragnehmer Wacker Neuson und dem Unterauftragnehmer Trackunit. Maßnahmen, die nur einen der Verarbeiter betreffen, sind entsprechend kenntlich gemacht.

Zugangskontrolle

Der Zugang zu allen Räumlichkeiten, in denen personenbezogene Daten verarbeitet werden, ist gesichert.

Zu den Maßnahmen gehören:

a) Alle wichtigen Einrichtungen verfügen über Zugangskontrolle.

b) Mitarbeiter erhalten Zugangsschlüssel /-karten.

c) Jede Person ist für den Schutz der Sicherheit ihres Schlüssels/ihrer Karte verantwortlich und wird Verluste oder Situationen, die die Gebäudesicherheit gefährden könnten, innerhalb von 24 Stunden melden.

d) Die Schlüssel/Karten dürfen nicht ausgeliehen, dupliziert, verändert oder verwendet werden, um unbefugten Personen Zugang zu Räumlichkeiten zu gewähren.

e) Es gibt aktive Alarmsysteme.

f) Besucher und Gäste müssen sich registrieren und werden in einem Protokoll erfasst.

g) Es wurde ein Due Diligence Programm für alle Kunden und Lieferanten etabliert, einschließlich derjenigen, die Zugang zu Räumlichkeiten haben, wie Reinigungsdienste und Wachpersonal.

h) Zugangskontrollen zu Sicherheitsbereichen minimieren potenzielle Bedrohungen für die Systeme durch Beschädigungen und Störungen.

i) Zugang zu Server-/Kommunikationsräumen sind auf autorisiertes Personal beschränkt.

j) Physische Datenträger werden in verschlossenen Schränken aufbewahrt.

Systemzugriff

Der Zugriff auf Datenverarbeitungssysteme ist nur für autorisierte, authentifizierte Benutzer möglich.

Zu den Maßnahmen gehören:

a) Die Benutzer der Dienste werden immer durch eindeutige Benutzernamen und Passwörter authentifiziert.

b) Der Zugang ist durch den Einsatz von VPN und ggf. MFA (Multifaktor-Authentifizierung) gesichert.

c) Ein Fernzugriff auf die Systeme wird Dritten zu keinem Zeitpunkt gewährt, es sei denn es liegt eine ausdrückliche Genehmigung vor. Wird dieser Zugang gewährt, wird dieser überwacht.

d) Die zur Verfügung gestellten Dienste werden durch Firewalls abgesichert und mittels Verschlüsselung für den nicht autorisierten externen Zugriff gesperrt.

e) Die von Trackunit betriebenen Dienste werden rund um die Uhr mit Tools zum kontinuierlichen Scannen von Schwachstellen überwacht, um ein Höchstmaß an Sicherheit zu gewährleisten.

f) Server und PC-Arbeitsplätze werden kontinuierlich mit Sicherheitsupdates versorgt, die vor böswilliger Nutzung von Schwachstellen in den verwendeten Anwendungen schützen.

g) Trackunit hat personenbezogene Daten (vollständiger Name, Benutzername, Passwort, E-Mail, etc.) an einen neuen Identity Management Provider übertragen. Diese Migration stellt sicher, dass personenbezogene Daten vollständig verschlüsselt bei einem hochmodernen Identitätsmanagement-Anbieter (okta.com) gespeichert werden, der nach SOC2 Typ1 und 2, ISO 27001, ISO27018 und CSA Star Level 2 zertifiziert ist.

h) Personen, die zum Zugriff auf die geschützten Teile der IT-Systeme berechtigt sind, erhalten von den IT-Administratoren ein spezielles Passwort. Das Passwort muss regelmäßig geändert werden und definierte Mindestanforderungen an Länge und Komplexität erfüllen.

i) Computer und andere Geräte müssen in Übereinstimmung mit den internen Richtlinien verwendet werden, z.B. müssen die Geräte nach dem Verlassen des Raumes gesperrt werden (Clear Screen Policy).

j) Bei Trackunit durchlaufen alle Entwickler ein obligatorisches Sicherheitstraining.

Datenzugriff

Die zur Nutzung von Datenverarbeitungssystemen berechtigten Personen erhalten nur Zugang zu den personenbezogenen Daten, zu denen sie berechtigt sind.

Zu den Maßnahmen gehören:

a) Die zur Verarbeitung personenbezogener Daten berechtigten Mitarbeiter wurden zur Vertraulichkeit verpflichtet oder unterliegen einer entsprechenden gesetzlichen Geheimhaltungspflicht.

b) Der Zugang von Mitarbeitern auf die Produktionssysteme, Entwicklungsumgebungen und Dienste ist auf diejenigen beschränkt, die für Erfüllung dienstlicher Zwecke erforderlich sind.

c) Der Zugang wird notwendigerweise geändert oder entfernt, wenn eine Person den Arbeitsplatz oder den Arbeitgeber wechselt.

d) Die interne IT-Abteilung führt regelmäßig Überprüfungen durch, um sicherzustellen, dass alle gewährten Rechte der Position des einzelnen Mitarbeiters entsprechen.

e) Niemandem wird Zugang zu IT Ressourcen gewährt, wenn er nicht geschult oder anderweitig angemessen über seine Sicherheitsaufgaben informiert ist.

Datenübermittlung

Personenbezogene Daten werden vor dem Lesen, Kopieren, Ändern oder Löschen durch Unbefugte während der Übertragung geschützt.

Zu den Maßnahmen gehören:

a) Das Trackunit RAW-Gerät verwendet den Advanced Encryption Standard (AES).

b) Die verschlüsselte Firmware wird von Trackunit IRIS zusammen mit einem sicheren Hash zur Authentizitäts- und Integritätsprüfung an die Geräte gesendet.

c) Die Kommunikation zwischen Diensten (Manager, Go, On) und IRIS ist als REST-Schnittstelle mit HTTPS-Verschlüsselung implementiert.

d) Die öffentliche Trackunit-API verwendet HTTPS-Verschlüsselung.

e) Die Kommunikation zwischen Trackunit RAW und IRIS basiert auf dem GSM-Netz und ist durch die GSM-Verschlüsselung geschützt. Für die Datenkommunikation wird ein proprietäres Protokoll auf IP/UDP verwendet. SMS werden gelegentlich für die Geräteverwaltung verwendet.

a) Die von den RAW-Geräten empfangene Kommunikation wird immer mit unterschiedlichen Mitteln validiert, um sicherzustellen, dass nur autorisierte Anfragen von den Geräten akzeptiert werden.

b) Zusätzlich zur GSM-Verschlüsselung wird Trackunit eine End-to-End-Verschlüsselung der m2m-Kommunikation zwischen Gerät und Cloud einführen.

Integrität und Verfügbarkeit

Diese Maßnahmen stellen sicher, dass personenbezogene Daten während der Verarbeitung vollständig und korrekt bleiben. Sie garantieren, dass personenbezogene Daten vor unbeabsichtigter Zerstörung oder Verlust geschützt sind, und dass eine rechtzeitige Wiederherstellung oder Verfügbarkeit personenbezogener Daten im Falle eines Vorfalls stattfinden kann.

Zu den Maßnahmen gehören:

a) Datenbanken werden täglich gesichert, um eine Systemwiederherstellung im Störungsfall zu ermöglichen.

b) Trackunit betreibt einen Incident Management Prozess mit 24/7-Überwachung kritischer Dienste.

c) Trackunit hat einen Incident Response Plan erstellt, der im Falle einer Verletzung befolgt werden muss. Er weist Verantwortlichkeiten zu und enthält einen Zeitplan für die beteiligten Personen, um die Meldefristen der DSGVO zu erfüllen. Dieser Incident Response Plan umfasst auch externe Kommunikation.

e) Lösch- und Aufbewahrungsfristen richten sich nach geltendem Recht.

Auftragsverarbeitungsvereinbarungen

Personenbezogene Daten, die im Auftrag des Kunden verarbeitet werden, werden ausschließlich in Übereinstimmung mit der jeweiligen Vereinbarung und den entsprechenden Weisungen des Kunden verarbeitet. Es wurde mit allen Gesellschaften, die Zugang zu personenbezogenen Daten haben können, Auftragsverarbeitungsvereinbarungen gemäß Artikel 28 DSGVO abgeschlossen.

Datentrennung

Personenbezogene Daten, die für verschiedene Zwecke erhoben werden, werden separat verarbeitet.

Zu den Maßnahmen gehören:

a) Die von den Geräten / Maschinen bezogenen personenbezogenen Daten werden automatisch den verschiedenen Kunden zugeordnet. Die Daten sind immer von den Kunden getrennt.

b) Der Kunde hat nur Zugang zu seinen eigenen personenbezogenen Daten.

c) Kundendaten werden stets vertraulich behandelt. Auditrechte, die Kunden ggf. eingeräumt werden, schließen immer das Recht oder die Möglichkeit aus, die Daten anderer Kunden einzusehen.

Compliance

Es wurden Prozesse für die regelmäßige Prüfung, Bewertung und Bewertung der Wirksamkeit technischer und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung etabliert.

a) Wacker Neuson SE hat einen Datenschutzbeauftragten (DSB) bestellt. Er steht für Fragen und Anliegen zur Datenverarbeitung unter datenschutz@wackerneuson.com zur Verfügung. Trackunit hat ebenfalls einen Datenschutzbeauftragten bestellt.

b) Die aufgestellten Grundsätze und Richtlinien zum Datenschutz werden jährlich überprüft und ggf. aktualisiert.

c) Es liegt eine Datenschutzfolgenabschätzung vor, um die Auswirkungen der Verarbeitungen auf den Schutz personenbezogener Daten gemäß Art. 35 DSGVO zu bewerten.

d) Es werden angemessene Schritte unternommen, um sicherzustellen, dass das Personal die in diesem Dokument beschriebenen technischen und organisatorischen Maßnahmen kennt und einhält. Alle Mitarbeiter müssen in angemessenen Zeitabständen Schulungen absolvieren, die vom DSB durchgeführt werden.

e) Trackunit führt jede zweite Woche ein Due-Diligence-Programm für alle Kunden und Lieferanten durch, um Risiken zu identifizieren.

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.