Data Processing Agreement

in accordance with Article 28 GDPR

between

Client

- Controller - hereinafter referred to as Client -

and

Wacker Neuson SE

- Processor - hereinafter referred to as Contractor -

1. Subject matter and duration of contract

(1) Subject matter

The Contractor processes the data specified in clause 2 (2) of this Agreement as part of the provision of Telematics Services for Customers (hereinafter "**Personal Customer Data**"). The subject matter of the contract is based on the customer's request for a Wacker Neuson Group EquipCare Account in connection with the EquipCare Terms & Conditions (hereinafter "**Service Agreement**").

(2) Duration

The contract lasts as long as the Service Agreement exists. The right to termination without notice for cause remains unaffected.

2. Precise definition of contract content

(1) The type and purpose of the proposed processing of Personal Customer Data

The type and purpose of the processing of Personal Customer Data by the Contractor for the Client are the provision of services in connection with Telematics Services, including geolocation, transmission and analysis of Machinery data, predictive maintenance and recommendations for action regarding Machinery use. **Annex 2** contains detailed instructions from the Client regarding the transmission of the Personal Customer Data to third parties. The Contractor also anonymises Personal Customer Data that are the subject of this Agreement on behalf of the Client. Anonymised data are not Personal Customer Data within the meaning of this Agreement. The Client has the right to use these anonymised data for its own purposes.

The provision of the contractually agreed data processing takes place (i) in a Member State of the European Union or in a State party to the Agreement on the European Economic Areas and/or (ii) in a third country if the special requirements under Article 44 et seqq. GDPR have been met.

(2) Type of data

The following types/categories of data are the subject of the processing of Personal Customer Data (list/description of the data categories)

☒ Customer master data (to the extent that the Contractor does not use these as controller)

☒ Log-in data (e-mail, password)

☒ Planning and control data

☒ Geolocation data

☒ Machinery data

(3) Categories of data subjects

The categories of data subjects affected by the data processing include:

☒ Employees of the Client and its affiliated enterprises within the meaning of the German Stock Corporation Act (*Aktiengesetz*)
☐ Employees of the Contractor and its affiliated enterprises within the meaning of the German Stock Corporation Act
☐ Employees of Distributors of the Contractor

3. Technical and organisational measures

(1) The Contractor must document the implementation of the technical and organisational measures set out and required prior to the contract being awarded before commencing processing, in particular with respect to the actual execution of the contract.

(2) The Contractor must with respect to its processing operations under this contract ensure the security pursuant to point (c) of Article 28, Article 32 GDPR, in particular in conjunction with Article 5(1) and (2). Overall, the measures to be taken are data security measures to ensure a level data security appropriate to the risk with respect to the confidentiality, integrity, availability and the resilience of the systems. In this respect, the state of the art, the implementation costs and the nature, scope and purposes of the processing as well as varying likelihood and severity of the risk for the rights and freedoms of natural person within the meaning of Article 32 (1) GDPR are to be taken into account. Specifically, the Contractor implements the measures set forth in **Annex 1**.

(3) The technical and organisational measures are subject to technical progress and further development. The Contractor is permitted to implement alternative adequate measures. The level of security may not be lower than that of the specified measures. Significant changes must be documented.

4. Rectification, restriction of processing and erasure of Personal Customer Data

(1) The Contractor may not rectify, erase or restrict the processing of Personal Customer Data autonomously, but only in accordance with documented instructions of the Client. If any data subject contacts the Contractor directly in this respect or due to the exercise of other rights of data subjects, the Contractor will forward this request to the Client.

(2) To the extent covered by the standard scope of the Telematics Services, the Contractor will support the Client in its compliance with the rights of data subjects in accordance with Clause 8 (2) of this Agreement.

5. Quality assurance and other obligations of the Contractor

In addition to compliance with the provisions of this contract, the Contractor also has statutory obligations pursuant to Articles 28 to 33 GDPR; the Contractor in this respect in particular warrants that it will comply with the following requirements:

a) Written appointment of a data protection officer, who performs his/her activities in accordance with Articles 38 and 39 GDPR. This person's current contact data are to be easily accessible on the Contractor's website.
b) Protection of confidentiality pursuant point (b) of Article 28(3), 29, 32(4) GDPR. The Contractor will when carrying out work only use employees who have been committed to confidentiality and familiarised beforehand with the data protection provisions relevant to them. The Contractor and any person acting under the authority of the Contractor, who has access to Personal Customer Data, may not process those data except on the documented instructions of the Contractor, unless required to do so contrary to these instructions by Union or Member State law. The Contractor will in such a case inform the Client of those legal requirements before the processing, unless that law prohibits such information on important grounds of public interest.
c) The Client and the Contractor will cooperate, on request, with the supervisory authority in the performance of its tasks.
d) Inform the Client without delay of control actions and measures taken by the supervisory authority insofar as they relate to this contract. This also applies if a competent authority investigates as part of administrative offence or criminal proceedings with respect to the processing of Personal Customer Data during processing by the Contractor.
e) Where the Contractor itself is subject to control by the supervisory authority, administrative offence or criminal proceedings, the liability claim of a data subject or a third party or any other claim in connection with the processing by the Contractor, it must, on request, provide the Client with adequate support.
f) The Contractor regularly checks its internal processes and the technical and organisational measures to ensure that the processing for which it is responsible is in compliance with the requirements of Article 28 GDPR.
g) Verifiability to the Client of the technical and organisational measures taken as part of its control powers pursuant to Clause 7 of this Agreement.

6. Subcontracting

(1) Subcontracting within the meaning of this provision means those services provided by "additional processors" within the meaning of Article 28(4) GDPR for the Contractor on behalf of the controller.

(2) The Client agrees to the engagement of the following subcontractors, subject to the condition of a contractual agreement pursuant to Article 28(2) to (4) GDPR:

Subcontractor company	**Country**	**Service**
Amazon (AWS)	Ireland, UK, Germany	"Off-site" storage and processing of Personal Customer Data
OKTA	Tenant "Europe"	Identity Management
Zitcom A/S	Denmark	"On-site" storage and processing of Personal Customer Data
Trackunit A/S	Denmark	Maintenance and development of the telematics services
Trackunit AB	Sweden	Maintenance and development of the telematics services
Trackunit AS	Norway	Maintenance and development of the telematics services
Trackunit B.V.	Netherlands	Maintenance and development of the telematics services

Trackunit GmbH	Germany	Maintenance and development of the telematics services
Trackunit Inc.	USA	Maintenance and development of the telematics services
Trackunit Ltd.	UK	Maintenance and development of the telematics services
Trackunit SAS	France	Maintenance and development of the telematics services

The engagement of additional subcontractors or the replacement of an existing subcontractor are admissible to the extent that:

- The Contractor notifies the Client of such engagement in advance, in writing or in text form, with a reasonable period of advance notice, and
- the Client does not within 10 (ten) business days of this notification object to the planned engagement to the Contractor in writing or in text form based on legitimate data protection grounds;
- this is based on a contractual agreement pursuant to Article 28(2) to (4) GDPR.

Any objection of the Client to any intended changes with respect to the engagement of an additional subcontractor or the replacement of an existing contractor is only admissible for good cause to be evidenced by the Contractor. Good cause only exists if the change is unacceptable to the Client taking into account all circumstances and balancing the interests of both parties. The Client can only raise an objection within a reasonable period (usually 2 (two) weeks) after having been informed of the change by the Contractor.

In the event of a admissible objection, the Contractor can terminate the Service Agreement, including this Data Processing Agreement, with effect at the point in time the Contractor commences the engagement of an additional subcontractor or the replacement of an existing subcontractor and wants to grant this subcontractor access to Personal Customer Data. The Contractor will indicate this date in the notification of the planned engagement of an additional subcontractor or replacement of an existing subcontractor.

(3) The disclosure of the Client's Personal Customer Data to the subcontractor and its first activities are only permitted when all requirements for subcontracting have been met.

(4) If the subcontractor provides the agreed service outside the EU/EEA, the Contractor ensures data protection reliability with appropriate measures. The Client hereby grants the Contractor the authorisation to enter into EU standard contractual clauses (controller-to-processor) on behalf of the Client as a "data exporter" with any subcontractors in third countries outside the European Economic Area. At the Client's request, the Contractor will present to the Client EU standard contractual clauses it has entered into on its behalf.

(5) Any further outsourcing by the subcontractor requires the explicit consent of the main contractor (at least in text form); all contractual provisions in the contractual chain are also to be imposed on the additional subcontractor.

7. Client's control rights

(1) The Contractor ensures that the Client can in accordance with clauses (2) and (3) convince itself of compliance with the Contractor's obligations pursuant to Article 28 GDPR. The Contractor undertakes

to provide the Client, upon request, with the necessary information and in particular to evidence the implementation of the technical and organisational measures.

(2) The evidence of such measures concerning the contract can, at the reasonable discretion of the Contractor, be provided by

- compliance with approved codes of conduct pursuant to Article 40 GDPR;
- certification in accordance with an approved certification process pursuant to Article 42 GDPR;
- current certificates, reports or report extracts from independent instances (e.g. auditors, internal audit, data protection officer, IT security department, data protection auditors, quality auditors);
- appropriate certification through an IT security or data protection audit (e.g. in accordance with BSI *(Federal Office for Information Security*) IT-Grundschutz (*baseline IT protection)*.

(3) If the Client is of the opinion that the evidence described in clause (2) is not sufficient or that a breach of this Agreement or the applicable statutory requirements exists, the Client has the right to carry out inspections through an independent third party ("auditor") commissioned by it in consultation with the Contractor and obliged by law or professional regulations to maintain secrecy or to have such inspections carried out by auditors to be appointed in each individual case. For this purpose, the Client has the right to convince itself of the Contractor's compliance with this Agreement in its business operations during normal business hours by means of spot checks, to be carried out by the auditor, which must be notified in good time (usually two (2) weeks prior to the planned inspection). Access to the Contractor's premises will take place exclusively in the constant presence of a representative of the Contractor. This representative has the authority to decide on the course of the inspection to the extent that this is necessary to prevent disruptions to the Contractor's operations and to maintain the Contractor's confidentiality obligations towards third parties.

(4) Business and trade secrets of the Contractor that become known to the Client during the course of such an inspection, are be treated by the Client as strictly confidential. Records of this may not be made unless this is absolutely necessary for the Client to exercise its control right.

(5) Regular on-site inspections by the Client in accordance with clause (3) are permitted at most once per calendar year. Additional inspections by the Client in accordance with clause (3) can only be carried out for good cause to be evidenced by the Client.

(6) The Contractor can request reimbursement on the reasonable costs incurred by it to facilitate inspections by the Client and to support the Client with these inspections, unless any deficiencies identified during the inspection are based on any culpable breach by the Contractor of this Agreement or the Client's instructions.

8. Support obligations of the Contractor

(1) The Contractor supports the Client in complying with the obligations specified in Articles 32 to 36 GDPR for the security of Personal Customer Data, notification obligations in the event of personal data breaches, data protection impact assessments and prior consultations. These include:

a) ensuring an appropriate level of security with technical and organisational measures that take the circumstances and purposes of the processing as well as the predicted likelihood and severity of any possible breach of rights due to security gaps and facilitate an immediate detection of relevant breach events

b) the obligation to notify the Client without undue delay about breaches of the availability, confidentiality or integrity of Personal Customer Data within the meaning of Article 33 GDPR
c) the obligation to support the Client in its obligation to inform the data subject and to provide it in this context with all relevant information without undue delay
d) supporting the Client with its data protection impact assessment
e) supporting the Client in prior consultations with the supervisory authority

(2) The Contractor will, if possible with appropriate technical and organisational measures, support the Client to the extent reasonable and necessary to meet its obligation to respond to requests for the exercise of the rights of data subjects with respect to their Personal Customer Data insofar as such requests concern the Personal Customer Data covered by this Agreement, in particular with respect to their rights under Articles 12 to 23 GDPR.

(3) The Contractor can claim remuneration for support services that are not included in the specifications or that are not based on any misconduct of the Contractor.

9. Client's authority to issue instructions

(1) The Client will confirm oral instructions without undue delay (at least in text form).

(2) The Contractor must inform the Client without undue delay if it is of the opinion that an instruction breaches data protection regulations. The Contractor has the right to suspend the execution of the corresponding instruction until it has been confirmed or amended by the Client.

10. Erasure and return of Personal Customer Data

(1) Copies or duplicates of Personal Customer Data will not be made without the Client's knowledge. Backup copies are excluded from this if they are required to ensure proper data processing, as are data required with respect to compliance with statutory retention periods.

(2) During the term of the Service Agreement and for up to 10 (ten) days after it ends, the Contractor will enable the Client to have the Contractor in accordance with the Client's request in text form transmit the Client's Personal Customer Data in a machine-readable format or erase them. After expiry of this period, the Contractor will, subject to clauses (3) and (4), erase Personal Customer Data of the Client existing in the services and hand over any other Personal Customer Data that have come into its possession, which the Contractor has received under this Data Processing Agreement or destroy such in compliance with data protection regulations following prior consent. This same applies to test and scrap material.

(3) The aforementioned erasure obligations do not apply

(i) to copies of Personal Customer Data stored on backup media and/or backup services until erasure thereof is provided for in accordance with recognised information security procedures, provided that the Contractor, subject to point (ii), does not use such stored data and documents for any purposes other than backup and the provisions of this Agreement with respect to this temporary storage continue to apply;

(ii) to the extent the Contractor is required by law to store the Personal Customer Data.

(4) The anonymisation of these data by the Contractor is equivalent to any destruction or erasure of Personal Customer Data.

(5) Documentation that serves to evidence that the data processing was in compliance with the contract and proper is to be retained by the Contractor beyond the end of this Agreement in accordance with the applicable retention periods. It can hand documentation over to the Client when the contract ends in order to discharge itself from this obligation.

11. Indemnification

(1) If third parties, in particular data subjects, assert claims against the Contractor on the basis of or in connection with the processing of Personal Customer Data that are the subject of this Agreement ("Third-Party Claims"), the Contractor can request that the Client assume the defence against the Third-Party Claims and indemnifies the Contractor against Third-Party Claims insofar as they have been established by a non-appealable judgment or have been settled or recognised with the consent of the Client. The Client must bear the costs in connection with the defence against or settlement of Third-Party Claims and reimburse the Contractor any such costs that it may incur. The same applies to any costs incurred by the Contractor due to any measures taken by supervisory authorities based on the processing of Personal Customer Data under this Agreement and in accordance with the Client's instructions.

(2) If the Contractor requires that the Client act in accordance with clause (1), the Contractor will leave sole control over the defence against Third-Party Claims in the internal relationship to the Client and support the Client to the extent reasonable with respect to the defence against these Third-Party Claims at the expense of the Client.

(3) The Client is not obliged to indemnify the Contractor in accordance with clause (1) if the Third-Party Claims result (i) from any breach of this Agreement by the Contractor or (ii) specifically from the anonymisation of the Personal Customer Data and the use of these anonymised data for the purposes of the Contractor.

12. Annexes

Annex 1: Technical and organisational measures

Annex 2: Specific instructions of Client regarding the transmission of Personal Customer Data to third parties

Annex 1

EquipCare – Technical and organisational measures

Physical access

Physical access to premises, where personal data may be processed, is protected.

Measures include:

a) All key facilities have physical access control.

b) Employees are issued access control keys/cards.

c) Each individual is responsible for protecting the security of his/her key/card and will report loss or situations that could possibly jeopardise building security within 24 hours.

d) The keys/cards cannot be: lent out, duplicated, altered, or used to give unauthorised personnel access to Trackunit premises.

e) Active alarm systems are in place.

f) Visitors and guests have to sign and will be registered in a protocol.

g) Due diligence programme for all customers and suppliers, including those accessing the premises, such as cleaning services and guards.

h) Physical access control to secure areas minimise potential threats to the Trackunit systems through damage and interference.

i) Access to server/communication rooms at the premises is restricted to authorised personnel.

j) Physical data are stored in a locked cabinet at the premises of the company.

System access

The access to data processing systems is only available for approved, authenticated users.

Measures include:

a) Users of the services are always authenticated by unique usernames and passwords, and access tokens are granted.

b) The access is secured through use of VPN and, where applicable, MFA (multi-factor authentication).

c) No remote access to systems will be given to third parties at any time unless specific authorisation is received. Such access, if granted, must be supervised at all times.

d) The service is kept secure and locked down for external access by firewalls to ensure that the system can only be accessed through encryption and authentication.

e) Trackunit services are monitored 24/7 with continuous vulnerability scanning tools to ensure the highest level of security.

f) On an on-going basis, updates on servers and PC workstations are deployed that protect against malicious use of vulnerabilities in the applications used.

g) Trackunit migrated personal data (full name, username, password, email, etc.) to a new Identity Management Provider. The migration ensures that personal data is stored fully encrypted at a state-of-the-art Identity Management provider (okta.com), which is SOC2 Type1 and 2, ISO 27001, ISO 27018 and CSA Star Level 2 certified.

h) Persons authorised to have access to the protected parts of the IT systems receive a special password from the IT administrators. The password must be changed on a regular basis and must fulfil defined minimum requirements regarding length and complexity.

i) Computers and other devices have to be used in accordance with the internal policies, for example the devices have to be locked after leaving the room.

j) At Trackunit, all developers go through mandatory security training.

Data access

Persons entitled to use data processing systems gain access only to personal data that they are authorised to access.

Measures include:

a) Internal measures ensure that employees authorised to process personal data have committed themselves to confidentiality or are under appropriate statutory obligation of confidentiality.

b) Access to services by staff is kept limited to those who need to access the production systems and development environments and services for professional purposes. User access to the IT systems will be granted only where access is necessary to perform the person's job.

c) Access will be modified or removed as found appropriate when a person changes job or leaves the employer.

d) Internal IT department performs regular verification to make sure that all the rights granted are equivalent to what is needed for the individual employee's position.

e) No individual will be given access to the IT network unless properly trained or otherwise adequately informed of his/her security responsibilities.

Data Transmission

Personal data is protected from being read, copied, altered or deleted by unauthorized parties during transfer.

Measures include:

a) The Trackunit RAW device utilises the Advanced Encryption Standard (AES).

b) The encrypted firmware is sent from IRIS to the devices together with a secure hash used for authenticity and integrity check.

c) Communication between services (Manager, Go, On) and IRIS is implemented as REST interfaces using HTTPS as encryption.

d) Trackunit public API is using HTTPS encryption.

e) Communication between Trackunit RAW and IRIS is based on the GSM network and protected by GSM encryption. A proprietary protocol on IP/UDP is used for the data communication. Text messaging is occasionally used for device management.

f) Communication received by the RAW devices is always validated by different means to ensure that only authorised requests are accepted by the devices.

g) In addition to GSM encryption, Trackunit is in the process of introducing end-to-end encryption of the m2m communication between device and cloud.

Integrity and Availability

These measures ensure that personal data remains complete and accurate while being processed. Personal data is protected from accidental destruction or loss, and there is timely access, restoration or availability to personal data in the event of an incident.

Measures include:

a) Databases are backed up on a daily basis to enable system recovery in case of incidents.

b) An incident management process is in place with 24/7 monitoring of critical services.

c) Trackunit drafted an incident response plan to be prepared in case of a breach. It allocates responsibilities and includes a time schedule for the involved people towards the notification requirements in the GDPR.

d) Erasure and retention periods are governed by applicable law.

Processing instructions

Personal data processed on behalf of the customer is processed solely in accordance with the relevant agreement and related instructions of the customer. There are Data Processing Agreements in place with all subsidiaries and entities that may have access to personal data, fulfilling the requirements of Article 28 GDPR.

Data Separation

Personal data collected for different purposes is processed separately.

Measures include:

a) Personal data received from the units / machinery is automatically assigned to the different customers. The data is always separated from the customers.

b) Customers have access only to their own personal data.

c) Customer data is always kept confidential. Audit rights given to customers always exclude the right or ability to look at the data of other customers.

Compliance

Processes established for the regular testing, assessing and evaluation of the effectiveness of technical and organisational measures for ensuring the security of the processing.

a) Wacker Neuson SE has appointed a Data Privacy Officer (DPO), who can be contacted for any questions or requests concerning data processing at privacy@wackerneuson.com. Trackunit also has appointed a DPO.

b) The established principles and guidelines on data protection are reviewed annually and updated if necessary.

c) A data protection impact assessment is available to evaluate the impact of the processing on the protection of personal data pursuant to Article 35 GDPR.

d) Appropriate steps are taken to ensure that personnel are aware of and comply with the technical and organisational measures described in this document. All personnel must undergo training at appropriate intervals, to be provided by the DPO.

e) Trackunit conducts every second week a due diligence programme for all customers and suppliers to identify risks.

Annex 2

Specific instructions of Client regarding the transmission of Personal Customer Data to third parties

In accordance with the Service Agreement, the telematics solution facilitates access to Personal Customer Data by the Contractor, other companies of the Wacker Neuson Group and the Client's Distributors (e.g. providing EquipCare Services at the Client's request or for product development).

Specifically, the following recipients are to be given access to the Personal Customer Data for their own business purposes described below:

Recipient	Specific own business purpose
Wacker Neuson SE	• Second level support (in response to specific support request from Client)
Production company (of Wacker Neuson Group) that produced the Machinery in question, from which the relevant Personal Customer Data were transmitted.	• Second Level Support (in response to specific support request from Client) • Product development • Review of any warranty or guarantee claims
Distribution company (of Wacker Neuson Group) that sold the Machinery in question, from which the relevant Personal Customer Data were transmitted, directly the Client, any other previous owner or otherwise as intermediary.	• First Level Support (in response to specific support request from Client) • Review of any warranty or guarantee claims
Dealer (distributor) that sold the Machinery in question, from which the relevant Personal Customer Data were transmitted, to the Client or any other previous owner.	• First Level Support (in response to specific support request from Client) • Review of any warranty or guarantee claims

The Client hereby instructs the Contractor to transmit Personal Customer Data by granting access rights to the aforementioned recipients for the purposes specified there to the extent that this is necessary individual aforementioned business purposes of these recipients. In this respect, these recipients each act as a controller within the meaning of Article 4(7) GDPR.

If the Contractor itself is a recipient of the relevant Personal Customer Data, the Contractor hereby undertakes to the Client to only process the Personal Customer Data for the aforementioned purposes and as best as possible to avoid the creation of any direct reference to any person. The Contractor also undertakes not to make any copies of Personal Customer Data, but to only process the Personal Customer Data in the portal (as defined in the Service Agreement) operated by the Client. This does not restrict the making of copies of anonymised data.