

Version: February 2025

# **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 continues. The right to extraordinary termination for good cause remains unaffected. If the provision of the processing services that are the subject of this Agreement has not yet been completed after termination of the Service Agreement, or if the Contractor is otherwise still processing Personal Customer Data after termination of the Service Agreement or termination of this Agreement, the term of this Agreement shall only end upon completion of the provision of the processing services and the complete deletion or return of the Personal Customer Data to the Client.

## **2. Precise definition of contract content**

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

The nature and purpose of the processing of Personal Customer Data by the Contractor for the Client includes raw data as well as back-end and front-end processing of machine and geolocation data for the purposes of fleet management, deployment planning and location identification for services. The processing includes personal customer data for the purposes of license management, identification, authentication and authorization of natural persons when using telematics services. Geolocation data is transmitted via all technically available means, such as GPS and Bluetooth. Depending on the type of device, the machine data includes operating hours, kilometers driven, battery voltage, serial number and fault diagnosis. Furthermore, this machine data can be processed at the request of the client in

order to provide recommendations for action in machine handling, such as engine adjustments due to extreme topographical situations.

**Appendix 2** contains detailed instructions of the Client with regard to the transfer of Personal Customer Data to third parties. In addition, the Contractor shall anonymize Personal Customer Data that is the subject of this Agreement on behalf of the Client. Anonymized data is not Personal Customer Data within the meaning of this Agreement. The Contractor is also entitled to use this anonymized 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 another state party to the Agreement on the European Economic Area and/or (ii) in the third countries identified in Annex 3 or in the respective notification of the commissioning of a further subcontractor or the change of an existing subcontractor in accordance with Section 6, if the special requirements of Art. 44 et seq. GDPR are fulfilled.

## (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
- 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 necessary technical and organizational measures set out in advance of the award of the contract before the start of processing, in particular with respect to the specific execution of the contract.
- (2) The Contractor shall establish security in accordance with Art. 28 para. 3 lit. c, 32 GDPR, in particular in conjunction with Art. 5 para. 1, para. 2 GDPR, in relation to its processing operations under this contract. Overall, the measures to be taken are data security measures and measures to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. The state of the art, the implementation costs and the

nature, scope and purposes of the processing as well as the different probability of occurrence and severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR must be taken into account. Specifically, the Contractor shall take the measures set out in **Annex 1**.

- (3) The technical and organizational measures are subject to technical progress and further development. In this respect, the Contractor is permitted to implement alternative adequate measures. In doing so, the security level of the specified measures may not be undercut. Significant changes must be documented.

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

The Contractor may not rectify, erase or restrict the processing of personal customer data autonomously, but only in accordance with documented instructions from the Client. If a data subject contacts the Contractor directly in this regard or to assert other data subject rights, the Contractor will pass this request on to the Client.

#### 5. Quality assurance and other obligations of the Contractor

In addition to complying with the provisions of this contract, the Contractor has legal obligations pursuant to Art. 28 to 33 GDPR; in this respect, the Contractor guarantees compliance with the following requirements in particular:

- a) Written appointment of a data protection officer who performs his or her duties in accordance with Art. 38 and 39 GDPR. Their current contact details are easily accessible on the contractor's website.
- b) Maintaining confidentiality in accordance with Art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 GDPR. When carrying out the work, the Contractor shall only use employees who have been obliged to maintain confidentiality and who have previously been familiarized with the data protection provisions relevant to them. The contractor and any person subordinate to the contractor who has access to personal customer data may only process this data in accordance with the documented instructions of the client, unless they are obliged to process it contrary to these instructions under the law of the EU or a member state of the EU. In such a case, the Contractor shall notify the Client of these legal requirements prior to processing, unless the law in question prohibits such notification due to an important public interest.
- c) The Client and the Contractor shall cooperate with the supervisory authority in the performance of their tasks upon request.
- d) Immediately informing the client of any inspections and measures taken by the supervisory authority insofar as they relate to this order. This shall also apply if a competent authority investigates the Contractor in the context of administrative offense or criminal proceedings relating to the processing of Personal Customer Data in the context of commissioned processing.
- e) If the client is subject to an inspection by the supervisory authority, administrative offense or criminal proceedings, a liability claim by a data subject or a third party or any other claim in connection with the commissioned processing at the contractor, the contractor must provide reasonable support upon request.
- f) The Contractor shall regularly monitor the internal processes as well as the technical and organizational measures to ensure that the processing in its area of responsibility as processor is carried out in accordance with the requirements of Art. 28 GDPR.
- g) Verifiability of the technical and organizational measures taken as part of its control powers in accordance with Clause 7 of this agreement.

#### 6. Subcontracting

- (1) Subcontracting relationships within the meaning of this provision are those services that "other processors" within the meaning of Art. 28 (4) GDPR provide for the contractor on behalf of the

controller, and the client agrees to the commissioning of the subcontractors listed in Annex 3, subject to a contractual agreement in accordance with Art. 28 (4) GDPR.

(2) The client agrees to the engagement of further subcontractors or the change of an existing subcontractor within the meaning of Art. 28 (2) GDPR. Such an engagement or change is permissible insofar as:

- the Contractor notifies the Client of such an assignment in writing or in text form in advance with a reasonable lead time and
- the client does not effectively object to the planned commissioning in writing or in text form to the contractor;
- a contractual agreement in accordance with Art. 28 (4) GDPR is used as a basis.

An objection by the Client to an intended change with regard to the commissioning of a further subcontractor or the change of an existing subcontractor shall only be effective if it is made for good cause to be proven to the Contractor. Good cause shall only be deemed to exist if the change is unreasonable for the client, taking into account all circumstances and weighing up the interests of both parties. Moreover, the objection shall only be effective if it is received by the Contractor within the period specified in the Contractor's notification. This period must be at least two (2) weeks from receipt of the Contractor's notification by the Client.

In the event of an objection, the Contractor may terminate the Service Agreement, including this Data Processing Agreement, with effect from the time at which the Contractor wishes to commence the commissioning of a further subcontractor or the change of an existing subcontractor and grant this subcontractor access to Personal Customer Data. The Contractor shall indicate this point in time in the notification of the planned commissioning of a further subcontractor or the change of an existing subcontractor. Die Weitergabe Personenbezogener Kundendaten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(3) If the subcontractor provides the agreed service outside the EU/EEA, the Contractor shall ensure the admissibility under data protection law by taking appropriate measures and shall inform the Client of this in Annex 3 or in the respective notification of the commissioning of a further subcontractor or the change of an existing subcontractor. Insofar as the cooperation of the Client is required to establish the admissibility of such transfers outside the EU/EEA under data protection law, the Client shall support the Contractor to the extent necessary upon request.

## 7. Control rights of the Client

(1) The Contractor shall ensure that the Client can satisfy itself of the Contractor's compliance with its obligations under Art. 28 GDPR in accordance with paragraphs (2) and (3). The Contractor undertakes to provide the Client with the necessary information upon request and, in particular, to provide evidence of the implementation of the technical and organizational measures.

(2) Proof of such measures relating to the order may, at the contractor's reasonable discretion, be provided in particular 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) The Client shall also have the right to carry out checks - including inspections - itself or have them carried out by an inspector commissioned by it. The Contractor shall facilitate and contribute to such inspections.
- (4) The Client shall inform the Contractor in good time, as a rule at least two (2) weeks in advance, of the performance of a review, including an inspection. In urgent exceptional cases to be proven and justified by the Client, the Client shall be entitled to carry out a review, including an inspection, without prior notice if the purpose of the inspection would otherwise be at risk.
- (5) As a rule, the Client shall carry out inspections during the Contractor's normal business hours.
- (6) Access to the Contractor's premises shall take place exclusively in the permanent presence of a representative of the Contractor. This representative shall have the authority to decide on the course of the inspection insofar as this is necessary to prevent excessive disruption to the Contractor's operations and to safeguard the Contractor's confidentiality obligations towards third parties.
- (7) Business and trade secrets of the Contractor that become known to the Client in the course of such an inspection shall be treated as strictly confidential by the Client. Records of this may not be made unless this is absolutely necessary for the exercise of the Client's right of inspection.
- (8) Regular on-site inspections by the client in accordance with paragraph (3) are generally permitted no more than once per calendar year. Additional inspections by the client in accordance with paragraph (3) may only be carried out for good cause to be proven by the client.
- (9) The Contractor may demand reimbursement of reasonable expenses incurred by it for enabling inspections by the Client and for supporting the Client in these inspections, unless any defects found during the inspection are due to a culpable breach by the Contractor of this Agreement, instructions of the Client or laws applicable to the Contractor.

## 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. Authority of the client 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 that the Contractor is obliged to store the Personal Customer Data under the law of the EU or a Member State of the EU.
- (4) The anonymization of personal customer data by the contractor is equivalent to its destruction or deletion.
- (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 3:**      Subcontractors

## Annex 1

### **Technical and organisational measures**

For the description of the basic technical and organizational measures of the subcontractor services Microsoft Azure and Amazon Web Service, including the measures for building security, as well as relevant certifications, please consult:

Microsoft Azure: <https://learn.microsoft.com/en-us/azure/security/>

Amazon Web Services: [https://aws.amazon.com/security/?nc1=h\\_ls](https://aws.amazon.com/security/?nc1=h_ls)

In addition, the following essential technical and organizational measures have been implemented to comprehensively ensure the security of the processing of personal customer data in EquipCare in accordance with Art. 32 GDPR:

#### (1) Pseudonymization of personal customer data (Article 32 (1) (a) GDPR)

- Separation of processing paths in back-end processing with and without personal data (complete anonymization).

#### (2) Encryption of personal customer data (Article 32 (1) (a) GDPR)

- State-of-the-art transport encryption, primarily for network protocols and interfaces (e.g. API).
- Warehouse encryption in backend processing for personal data, primarily in the context of identity management.

#### (3) Ability to ensure the confidentiality of processing systems and services on a permanent basis (Article 32 (1) (b) GDPR)

- Employees with authorized access to personal customer data are obliged to maintain confidentiality and receive regular training.
- Use of a multi-level, up-to-date anti-malware system.
- Access controls and role concept based on the principles of “least privilege”, “need-to-know” and “segregation of duty”.
- Separation of technical and content-related operation of the telematics solution.
- Physical access restrictions to server and communication rooms.
- External parties are registered, recorded in a log and permanently monitored.

#### (4) Ability to ensure the integrity of processing systems and services over time (Article 32 (1) (b) GDPR)

- Logging of all accesses, changes and deletions with individual user names.
- Role concept for controlling authorizations (e.g. reading, writing, managing data).
- Use of VPN connections and e-mail transport encryption.
- Encryption and authenticity check of the firmware in the telematics modules.

#### (5) Ability to ensure the availability of processing systems and services on a continuous basis (Article 32 (1) (b) GDPR)

- Implementation of a standard backup and recovery concept to prevent the loss of data.



- Multi-level anti-virus and firewall concept with regular updates.
  - 24/7 monitoring of critical services.
  - Regular tests to check data recovery and documentation of the results.
- (6) Ability to ensure the resilience of processing systems and services over time (Article 32 (1) (b) GDPR)
- Implementation of processes for continuous monitoring, detection and response to security vulnerabilities.
  - Regular review of vulnerability warnings and implementation of penetration tests.
- (7) Ability to rapidly restore the availability of and access to Customer Personal Data in the event of a physical or technical incident (Article 32 (1) (c) GDPR)
- Regular tests to check data recovery and documentation of the results.
  - Safe storage of backup media in separate fire compartments.
  - Implementation of an intrusion detection system (IDS).
  - Creation and maintenance of emergency and alternative plans.
  - 24/7 monitoring of critical services.
- (8) Procedures for regular review, assessment and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing (Article 32 (1) (d) GDPR)
- Regular checks on the safety of the processing environment..
  - Regular review of the concept and documentation basis.
  - Regular training for employees with authorized access to personal customer data.
  - Central documentation of all data protection procedures and regulations with access for employees.
  - Embedding processing activities in the security, risk management and business continuity frameworks with a continuous improvement process.
  - Documented procedure for dealing with security incidents.

**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:

<b>Recipient</b>	<b>Specific own business purpose</b>
<b>Wacker Neuson SE</b>	<ul style="list-style-type: none"> <li>• Second level support (in response to specific support request from Client)</li> </ul>
<b>Production company</b> (of Wacker Neuson Group) that produced the Machinery in question, from which the relevant Personal Customer Data were transmitted.	<ul style="list-style-type: none"> <li>• Second level support (in response to specific support request from Client)</li> <li>• Product development</li> <li>• Review of any warranty or guarantee claims</li> </ul>
<b>Distribution company</b> (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.	<ul style="list-style-type: none"> <li>• First level support (in response to specific support request from Client)</li> <li>• Review of any warranty or guarantee claims</li> </ul>
<b>Dealer</b> (distributor) that sold the Machinery in question, from which the relevant Personal Customer Data were transmitted, to the Client or any other previous owner.	<ul style="list-style-type: none"> <li>• First level support (in response to specific support request from Client)</li> <li>• Review of any warranty or guarantee claims</li> </ul>

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..

**Annex 3**  
**Subcontractors**

Raw data processing of machine and geolocation data			
Company Subcontractor	Address/Country	Service	Information on appropriate safeguards for data transfers to a third country
Trackunit ApS	Gasværksvej 24, 9000 Aalborg, Denmark	Raw data processing of telematics services including geolocation data	
Trackunit ApS commissions corresponding subcontractors, which can be found in the following source:  <a href="https://content.trackunit.com/hubfs/PDF%20Assets/Legal%20Documents/Trackunit%20%7C%20Privacy%20%7C%20Sub%20Processor%20List%20%7C%202021-11%20%7C%20EN.pdf">https://content.trackunit.com/hubfs/PDF%20Assets/Legal%20Documents/Trackunit%20%7C%20Privacy%20%7C%20Sub%20Processor%20List%20%7C%202021-11%20%7C%20EN.pdf</a>			Standard Contractual Clauses / SCC (EU)

Back-end processing of machine and geolocation data including personal customer data			
Company name Subcontractor	Address/country	Service	Information on appropriate safeguards for data transfers to a third country
Wacker Neuson Beteiligung GmbH	Flughafenstr. 7 4063 Hörsching, Austria	Technical operation of the Microsoft Azure Tenant and its resource groups	
Wacker Neuson Produktion GmbH & Co. KG	Münchner Straße 31, 85084 Reichertshofen, Germany	Technical operation of the resource groups belonging to the telematics services	
Wacker Neuson Aftermarket & Services GmbH	Preußenstraße 41, 80809 Munich, Germany	License management for telematics services, product development and support for	

		telematics services and market analyses	
Microsoft Ireland Operations, Ltd.	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland	Raw data processing of telematics services including geolocation data, further processing such as sorting, storing, visualizing, transmitting; processing on servers in the Europe/West region	
Microsoft commissions corresponding subcontractors, which can be found in the following source: <a href="https://servicetrust.microsoft.com/DocumentPage/badc200c-02ab-43d9-b092-ed9b93b9b4a8">https://servicetrust.microsoft.com/DocumentPage/badc200c-02ab-43d9-b092-ed9b93b9b4a8</a>			For the USA: Adequacy decision or EU-U.S. Data Privacy Framework  For other third countries: Standard Contractual Clauses / SCC (EU)
SAP SE	Dietmar-Hopp-Allee 16 69190 Walldorf Germany	Processing of personal customer data for the purposes of identification, authentication and authorization of natural persons (identity management); processing on servers in the Europe region	
SAP SE commissions further subcontractors. The current list of SAP SE subcontractors can be requested from the Contractor.			

Front-end data processing			
Company name Subcontractor	Address/country	Service	Information on appropriate safeguards for data transfers to a third country
OneStop Pro Software Solutions GmbH	Tittlinger Str. 39, DE-94034 Passau, Germany	Operation, maintenance and development of front-end telematics services	
OneStop Pro Software Solutions GmbH. commissions further subcontractors. The current list of subcontractors of OneStop Pro Software Solutions GmbH. can be requested from the contractor.			