RSP CONNECT PRIVACY NOTICE

This privacy notice provides information on the processing of personal data in connection with the RSP Connect telematics service, supplementing the general privacy notice of RSP GmbH & Co. KG ("RSP") available at and . Detailed information regarding your data protection rights under the GDPR can be found in the general privacy notice.

The purpose of the RSP Connect Privacy Notice is to inform you about all activities relating to data processing at RSP Connect.

I. What is RSP Connect?

(1) RSP GmbH & Co. KG equips vehicles at the factory with a combined mobile communications module (SIM card with 4G modem) and telemetry module (GPS receiver, CAN bus-based function control and machine data acquisition), also referred to as the CU. Internet connectivity enables the centralised analysis and provision of machine and location data collected in the vehicle, as well as the control of functions and remote diagnosis and maintenance of the superstructures, provided the customer requests these services.

(2) These functions (geolocation of the end customer's vehicles, analysis of machine data, and the activation/deactivation of vehicle functions) are provided to the end customer for vehicle and fleet management via a web portal and a mobile app (together 'RSP Connect') by RSP GmbH & Co. KG. To this end, the individual vehicles transmit the necessary telemetry data to RSO.

II. What data is processed?

(1) When end customers and their end users use RSP Connect, RSP processes the following data:

- Vehicle information: e.g. Vehicle Identification Number (VIN), the vehicle model;
- Machine data from RSP superstructures: e.g. speeds, pressures, functions and their operating times, signal strengths of the radio module;
- User profile data from the web portal: e.g. name and email address of the connected user;
- Location information : minute-by-minute GPS coordinates of the vehicle, which were extracted to determine the location of the vehicle of registered end customers – even if the end customer's vehicle has been stolen;
- Journey information: e.g. driving speed, average speed, distance travelled, and the duration of journeys and parking periods for the vehicle of registered end customers;
- Control data: e.g. activated or deactivated functions of the RSP superstructures, error codes;
- Pseudonymous location information: GPS data extracted to determine the region of use of RSP vehicles as soon as RSP systems are in use;
- Contract data: e.g. subscription status, company name and address, as well as the name and contact details of the contact person (main user);
- Usage and user data: e.g. username and password, assigned roles and rights in the web portal, user activities including timestamps and accessed resources or events, access status / HTTP status code;
- Device data: e.g. IP addresses, session ID, start and end of session, browser version, app version information, IDs, network status information and internet service provider, device type/manufacturer/model, OS name/version, app name/version, library/SDK version, screen/UI parameters, URL/path/title, referrer URL;
- Survey data: e.g. when end customers provide feedback to the RSP. This may be done anonymously.

III. For what purposes is the data processed and on what legal basis?

(1) Provision of the RSP Connect service via the web portal or the app.

In order to use the web portal, the end customer must first agree to the End User Agreement for RSP Connect on the web portal. The legal basis for the processing of personal data by RSP GmbH & Co. KG, which may be necessary for the contractual provision of vehicle and fleet management services, is Article 6(1)(b) of the GDPR , whereby RSP acts as the end customer's data processor. Specific purposes of processing include, amongst others:

(i) **User management**
User management by the end customer to control access rights within RSP Connect,

(ii) **Provision of location-based functions**
Google Maps and Apple Maps are used as external media to provide location-based functions such as route navigation and the display of geographical information.

These services are provided by the following third-party service providers:

Google Maps: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland ("Google").

Apple Maps: Apple Inc., One Apple Park Way, Cupertino, California, USA ("Apple").

When using these services, information may be transmitted from your device to the respective providers. This may include:

Google Maps: IP address, GPS data and device location

Apple Maps: IP address, approximate location data, GPS data and interaction details (e.g. navigation routes). Data is only transmitted when you actively use functions that require map services, such as navigation.

Further information can be found here in the respective privacy policies:

Android: https://policies.google.com/privacy
iOS: https://www.apple.com/de/legal/privacy/

(iii) **Provision of maintenance confirmation workflows**
The digital signature (a representation of the user's handwritten input) and associated metadata (e.g. timestamp, user who confirmed, and context of the confirmation) are processed for verification purposes.

(iv) **Monitoring of Suction Excavator machine functions**
To track the vehicle condition and machine parameters used when operating RSP superstructures, to monitor distances travelled using route information and location data, and for theft protection.

(v) **Analytics services: Google Firebase Crashlytics, Twilio Segment, Mixpanel**
The app uses the analytics services Google Firebase Crashlytics, Twilio Segment and Mixpanel on the basis of your consent. We use these to collect pseudonymous user and usage data regarding the use of the app and web portal, specifically in relation to system crashes and errors for the purpose of error detection and resolution (Crashlytics), as well as certain user-triggered events (Twilio Segment and Mixpanel) to optimise the web portal and the RSP Connect app. The service providers act as data processors in this context.
Please note that this also involves the processing of pseudonymous but personal data in the so-called third country, the USA, i.e. outside the EEA. The European Commission has (within the framework of the so-called EU-US Transatlantic Data Privacy Framework) recognised the level of data protection for certain companies from the USA as adequate in its decision of 10 July 2023 pursuant to Article 45 of the GDPR. Google LLC, Mixpanel, Inc. and Twilio, Inc. are certified under the DPF, meaning that the adequacy decision applies.

(vi) For Crashlytics, information regarding device data and user data (including, amongst other things, error messages) is collected, primarily relating to the user's software and hardware. For the other analytics services, when the user performs a specific action, an identifier corresponding to the event – the instance ID of your device – is sent to Google.

You can deactivate the analytics services Firebase Crashlytics, Segment and Mixpanel at any time, thereby withdrawing your consent to the collection of this data with effect for the future. To do so, open the settings and click on "Deactivate".

(vii) **Push notifications**
We also use the Firebase Cloud Messaging service from Google Inc. for Android and Apple Push Notifications for iOS to send push notifications or so-called in-app messages (messages that are only displayed within the respective app) to your device. In doing so, Firebase and Apple generate a calculated key comprising the app's identifier and your device's identifier. This key is stored on our push platform alongside the settings you have selected, so that we can provide you with content in accordance with your preferences. The Firebase and Apple servers cannot draw any conclusions about user requests or determine any other data relating to an individual. Firebase and Apple act solely as transmitters.

Push notifications can be disabled and re-enabled at any time in the device settings. We do not process any personally identifiable data in this process.

(2) RSP uses machine data and control data for research, development and analysis purposes on the basis of legitimate interest (Article 6(1)(f) of the GDPR) in order to improve RSP products and customer services and to develop new machine functions; where possible, this data is pseudonymised or anonymised for statistical analysis. In addition, RSP processes the machine data to fulfil its product monitoring and safety obligations.
Location data is processed by RSP for statistical analyses of usage regions, for the planning and expansion of the service partner network, but also to assist the end customer with any investigations in the event of theft or loss during transport.

(3) RSP and the end customer process machine data in order to derive machine-specific service intervals, which, for example, trigger invitations to service inspections by authorised specialist workshops (personalised customer service) or make claims for rectification of defects objectively verifiable.

(4) RSP may process this data to comply with a legal obligation, to cooperate in police investigations and to protect RSP's rights to the extent necessary to respond to legal claims (including the disclosure of information in connection with legal proceedings) and to cooperate in police investigations concerning RSP vehicles.

(5) RSP may provide end customers with the opportunity to leave feedback on the web portal.

IV. Who is the data controller and to whom can I assert my rights?

(1) End customers registered on the web portal process the machine, location and control data provided for their own purposes as data controllers within the meaning of Article 4(7) of the GDPR. In particular with regard to other users of their vehicles, the data processed on the web portal may be considered personal data insofar as, for example, the territorial and material scope of the GDPR applies.

RSP GmbH & Co. KG, as the operator of the web portal for RSP Connect, processes the types of data listed under Section II (1) on behalf of the end customer in its capacity as the end customer's data processor. To this end, both parties have entered into a corresponding agreement in accordance with Article 28 of the GDPR.

(2) With regard to the data processed by RSP in accordance with Section III(2), both parties are considered joint controllers. Both parties have entered into a corresponding agreement in accordance with Art. 26 GDPR, in which they have also set out their obligations regarding the exercise of data subjects' rights. The point of contact for data subjects is the end customer. Data subjects may, however, exercise their

rights under Chapter III of the GDPR against both RSP and the end customer (as a rule, the end customer is the employer or a lessor of these RSP vehicles).

(3) How can you contact RSP?

RSP GmbH & CO. KG
Zum Silberstollen 10
07318 Saalfeld/Saale
Germany
Telephone +49 36 71 57 21 0
Fax +49 36 71 57 21 21
Email: info@rsp-germany.com

If you have any further questions regarding this privacy policy, please feel free to contact RSP's Data Protection Officer. You can reach our company Data Protection Officer using the contact details above, for the attention of the Data Protection Officer, or by email at datenschutz@rsp-germany.com

(4) Further information on data protection at RSP GmbH & Co. KG and the rights of data subjects under the GDPR is available at www.rsp.com/datenschutz

IV. Which recipients receive data?

(1) Other recipients of this data, in addition to the two parties, are RSP's contracted service providers (the web portal host, software manufacturer Proemion GmbH, Twilio Inc., Mixpanel Inc., Google Ireland Ltd.).

VI. Duration of storage

(1) RSP processes any personal data for as long as required for the aforementioned purposes. This means that RSP stores your personal data until the customer requests RSP to delete their account, or an end customer stops individual data processing operations, or RSP has anonymised the data.

(2) In the event of a legal claim, longer retention periods may apply. In such cases, the relevant data will be retained as required by law or for the duration of the claim.

(3) RSP will process anonymised data for extended periods, including for the purpose of developing new vehicles and for research and analysis purposes, and also to improve RSP Connect.

VII. Updates to this Privacy Notice

(1) This privacy notice may be updated. We will update the date at the top accordingly and recommend that you check this document regularly for changes.

Appendix

Processing of personal data under the EU General Data Protection Regulation

This appendix describes how RSP processes so-called product data and associated service data generated through your use of an RSP vehicle and the RSP Connect service.

A detailed overview of the data we have currently identified as product data and associated service data can be found in the *mandatory information under the EU Data Protection Regulation* regarding *RSP-Connect's connected products and associated services*, which is available at connect.rsp.com.

RSP treats all product data and associated service data as personal data, as it is inextricably linked to you as the data subject via your user account. Accordingly, its processing must always be carried out in accordance with applicable data protection laws, including the GDPR.

Scope and Definitions

1.1 This Annex governs the processing of personal data that also qualifies as product data and/or associated service data, which may be lawfully requested in accordance with

1.1.1.1 Chapter II of the EU Data Regulation (either directly from you or via third parties) or

1.1.1.2 Chapter V of the EU Data Regulation (by public authorities).

1.2 For the purposes of this Annex, the following definitions apply:

1.2.1.1 Main User: A natural or legal person who is registered with RSP as the owner of an RSP vehicle and/or is the main account holder in RSP Connect.

1.2.1.2 Other User: A natural or legal person who is contractually authorised to use the RSP vehicle on a temporary basis and/or is contractually authorised to use RSP Connect on a temporary basis.

1.2.1.3 User: A Primary User and/or an Other User.

1.2.1.4 Product data: Data generated through the use of the connected product and designed by the manufacturer to be accessible via an electronic communication service, a physical connection or in-device access.

1.2.1.5 Connected Service Data: Data resulting from the digitisation of user actions or processes relating to the RSP vehicle, which has been either intentionally recorded by you or generated as a by-product during the provision of a connected service via the app.

Lawful processing

RSP typically processes Product Data and Connected Service Data as set out in the RSP Connect Privacy Notice above. In cases where RSP is obliged to provide Product Data and Connected Service Data that also qualify as personal data, three main scenarios must be distinguished:

1.3 **The data subject is the requesting user:** We may be required to provide product data and associated service data, which also qualify as personal data, to a user who is also the data subject (in accordance with Article 4(1) or to a third party in accordance with Article 5(1) of the EU Data Protection Regulation). In such a case, the legal basis for processing the data is Article 6(1)(c) of the GDPR, as this is necessary to comply with a legal obligation (Article 4(1) and Article 5(1) of the EU Data Protection Regulation) to which RSP is subject. RSP complies with the data subject's instructions if the data subject exercises their right under Article 4(1) of the EU Data Protection Regulation or has selected a third party as the recipient of the data in accordance with Article 5(1) of the EU Data Protection Regulation.

1.4 **The data subject is not the requesting user:** If a user submits a request under Article 4(1) of the EU Data Protection Regulation or Article 5(1) of the EU Data Protection Regulation, or if a third party submits a request on behalf of the user in accordance with Article 5(1) of the EU Data Protection Regulation, without the requesting user also being the data subject in relation to the data that is the subject of such a request, the following applies:

1.4.1 If we know that the requesting user is not the data subject , we shall require the requesting user or the requesting third party, in accordance with Article 5(1) of the EU Data Protection Act, to provide evidence that the data subject has given their consent (Article 6(1)(a) of the GDPR).

1.4.2 If we have no grounds or reasons to believe that the requesting user is not the data subject, we must rely on the fact that the requesting user or the requesting third party has verified, in the scenarios set out in Article 5(1) of the EU General Data Protection Regulation, that their access to the requested available data is in accordance with the GDPR. Before we make product data and associated service data, which also qualify as personal data, available, we generally require enquirers to confirm their commitment to complying with the GDPR by accepting the General Terms and Conditions for the RSP-Connect telematics system provided by RSP, in particular with regard to its provisions concerning the EU Data Protection Regulation.

1.5 **Requests from government institutions, bodies and other authorities:** Granting access to public authorities, the Commission, the European Central Bank or a Union body that demonstrate the exceptional necessity of using certain data, as described in Article 15 of the Data Regulation – the scenario under Article 14(1) of the EU Data Regulation: In such cases, the legal basis for processing is Article 6(1)(e) of the GDPR, as the provision of product data and associated service data, which also qualify as personal data, is necessary to respond to a public emergency, whereby the emergency response and resolution are in the public interest.

1.6 **Procedure for requesting product data and/or associated service data under the EU Data Regulation**

1.6.1 Requests made under the EU Data Protection Regulation must clearly state the basis on which they are made:

1.6.1.1 GDPR (e.g. access, rectification) or

1.6.1.2 EU Data Regulation (e.g. access to product data and/or associated service data).

1.6.2 The main user is responsible for ensuring that other users (e.g. alternating users, other users in the case of shared user accounts) are aware of this RSP CONNECT privacy notice and consent to the transfer of data generated during the use of the connected product or the provision of connected service data. RSP assumes that all processed data relates to the main user, unless otherwise stated.

1.6.3 Requests under the EU Data Protection Regulation made by another user require verification as to whether this natural or legal person qualifies as a user. Where necessary, the verification may include the following:

1.6.3.1 Valid identification document (e.g. passport, identity card);

1.6.3.2 Documents proving a contractual right to the temporary use of the RSP vehicle and/or RSP Connect linked to the main user;

1.6.3.3 Details of the specific periods during which the Other User used the RSP vehicle and/or RSP Connect;

1.6.3.4 A written declaration (in text form is sufficient) that the request relates exclusively to data generated during the Other User's own use of the RSP vehicle or RSP Connect, or, in scenarios involving multiple users, a written declaration (in text form is sufficient) regarding the consent of other affected persons during the application period, possibly including the main user.