Declaration of self-commitment

(Declaration of unilateral commitment)

by

Rosenbauer International AG

Paschinger Strasse 90, 4060 Leonding, Austria

as Order Processor (hereinafter referred to as the “Contractor”) on the one hand

vis-à-vis their

RDS Connected Fleet client

as the Data Controller (hereinafter referred to as the “Principal”) on the other hand

Preamble

According to the provisions of Art. 28 GDPR, processors and controllers have entered into a contract (or another legal instrument in accordance with Art. 28 (3) GDPR) to ensure the processing of personal data in accordance with data protection law.

By this declaration of self-commitment, the processor makes the unilaterally binding declaration to its contractual partner, the principal, to comply with the following obligations within the scope of the data processing. This unilateral declaration does not impose any obligations on the data controller.

I. Subject of the declaration of commitment

(1) The contractor shall provide the principal with services in the area of the provision of Digital Solutions and RDS Connected Applications for the purpose of digital support of emergency crews (hereinafter "Main Contract") on the basis of a main contract. In this context, the contractor shall obtain access to personal data with regard to which it undertakes to process such data exclusively on behalf of and in accordance with the instructions of the principal. The scope and purpose of the data processing by the contractor shall result from the main contract, unless specified in more detail above; the examination of the permissibility of the data processing shall be the sole responsibility of the principal.

(2) The obligations under this declaration of commitment relate to all activities in connection with the main contract and in the course of which the contractor and its employees or persons appointed by the contractor come into contact with personal data originating from the principal or collected for the principal.

II. Categories of processed data and data subjects

(1) In the course of the performance of the main contract, the contractor shall have access to the categories of personal data listed below:

Contact data, geolocation data, log files in the system, operational information, logbook entries, fault and maintenance information, equipment and vehicle data (e.g. holder data), drone information, video data.

(2) The categories of data subjects are:

Employees and volunteers of the data controller, victims of disasters and other emergencies, third parties involved in the operation and employees of the data controller.

III. Right of instruction of the principal

(1) The contractor undertakes to collect, process or use data exclusively within the scope of the main contract and in accordance with the principal's express instructions; this also applies to the transfer of personal data to a third country or to an international organisation. If the contractor is obliged to carry out further processing under the law of the European Union or a member state to which it is subject, it undertakes to notify the principal of this prior to processing.

(2) The contractor undertakes to comply with any instructions permissibly issued by the principal in writing, whereby this also includes instructions on how to correct, delete and block data. Instructions issued shall be documented in writing by the contractor.

(3) If the contractor is of the opinion that an instruction of the principal violates data protection regulations, it shall notify the principal thereof immediately and shall in this case suspend the implementation of this instruction until it is confirmed or amended by the principal. The contractor shall refuse to carry out an obviously illegal instruction.

IV. Control rights of the principal

(1) The contractor declares to grant the principal the right at any time to inspect the contractor's technical and organisational measures at the principal's expense prior to the commencement of data processing and thereafter on a regular basis. Within this framework, the principal may personally inspect the technical and organisational measures of the contractor after timely coordination during normal business hours or have them inspected by a competent third party, provided that this third party is not in a competitive relationship with the contractor.

(2) The contractor undertakes to provide the principal, upon the principal's oral or written request and within a reasonable period of time, with all information and evidence required to carry out a check of the contractor's technical and organisational measures.

(3) The contractor undertakes to rectify within a reasonable period of time any errors or irregularities which the principal discovers, in particular during the examination of the results of the order, and of which the principal informs the contractor.

V. The contractor's data protection measures

(1) The contractor undertakes to comply with the statutory provisions on data protection and not to disclose information obtained from the principal's domain to third parties or to expose it to third party access. Documents and data shall be secured against unauthorised access, taking into account the state of the art.

(2) The contractor undertakes to design the internal organisation in their area of responsibility in such a way that it meets the special requirements of data protection. They shall take all necessary technical and organisational measures to adequately protect the principal’s data in accordance with Art. 32 EU GDPR, but at least the measures for access control, admission control, authorisation control, transfer control, input control, order control and availability control listed in Annex **./1**.

The contractor reserves the right to change the measures taken, provided that it ensures that it does not fall short of the level of protection assured to the principal. In the event of significant changes, the contractor undertakes to inform the principal.

(3) The persons employed by the contractor for data processing are prohibited from collecting, processing or using personal data without authorisation. The contractor therefore undertakes to ensure that all persons entrusted by them with the processing and fulfilment of the main contract (hereinafter referred to as "employees") are informed accordingly in accordance with Art. 28 (3) (b) of the EU GDPR to confidentiality and to exercise due diligence to ensure compliance with this obligation.

The contractor undertakes to ensure that these obligations continue after the termination of this contract or the employment relationship between the employee and the contractor. The contractor undertakes to provide the principal with appropriate proof of the obligations upon request.

VI. Information obligations of the contractor

(1) In the event of an audit of the contractor by the data protection authority, suspicion of data protection violations or breaches of contractual obligations by the contractor, suspicion of security-related incidents or other irregularities in the processing of personal data by the contractor, by persons employed by it within the scope of the contract or by third parties, the contractor undertakes to inform the principal immediately in writing and to provide at least the following information:

a) a description of the nature of the personal data breach, including, where possible, the categories and the number of data subjects concerned, the categories concerned and the number of personal data records concerned;

b) a description of the measures taken or proposed by the contractor to remedy the breach and, where appropriate, measures to mitigate its possible adverse effects.

(2) The contractor undertakes to immediately take the necessary measures to secure the data and to mitigate possible adverse consequences for the data subjects, as well as informing the principal about this and requesting further instructions from them.

(3) The contractor also undertakes to provide the principal with information at any time, insofar as the principal's data is affected by a request pursuant to VIII (1).

(4) Should the principal’s data at the contractor be endangered by events or measures of third parties of whatever kind, the contractor undertakes to inform the principal thereof immediately, unless it is prohibited from doing so by a court or official order. In this context, the contractor shall immediately inform all competent bodies that the decision-making authority over the data lies exclusively with the principal as the “data controller” within the meaning of the EU GDPR.

(5) The contractor and, where applicable, their representative shall keep a list of all categories of processing activities carried out on behalf of the principal, which shall include all information pursuant to Art. 30 (2) of the EU GDPR. The list shall be made available to the principal on request.

(6) The contractor undertakes to cooperate to a reasonable extent in the preparation of the procedure directory by the principal and to provide the principal with the respective required information in an appropriate manner at the principal's expense.

VII. Use of subcontractors

(1) The contractor undertakes to perform contractually agreed services in whole or in part only with the involvement of such subcontractors as it has carefully selected according to their suitability and reliability and has committed them in accordance with the provisions of this contract. The contractor further undertakes to ensure that the principal can also exercise their rights under this contract (in particular its audit and inspection rights) directly against subcontractors and shall notify the principal immediately prior to any such assignment and name the intended subcontractor in order to give the principal the opportunity to object to the use of a subcontractor.

(2) If subcontractors in a third country are to be involved, the contractor undertakes to ensure that an appropriate level of data protection is guaranteed at the respective subcontractor and to prove this to the principal upon first request.

(3) A subcontractor relationship within the meaning of these provisions does not exist if the contractor engages third parties to provide services that are to be regarded as pure ancillary services. This includes, for example, postal, transport and shipping services, cleaning services, telecommunications services without any specific reference to services provided by the contractor to the principal and guarding services. Maintenance and testing services constitute subcontractor relationships within the meaning of these provisions insofar as they are provided for IT systems that are also used in connection with the provision of services for the principal.

VIII. Requests and rights of data subjects

(1) The contractor undertakes to support the principal as far as possible with suitable technical and organisational measures in the fulfilment of the principal's obligations pursuant to Art. 12–22, as well as 32 and 36 of the EU GDPR.

(2) If a data subject asserts rights directly against the contractor, such as the right to information, correction or deletion with regard to their data, the contractor shall not react independently, but shall immediately refer the data subject to the principal and await the latter's instructions.

IX. Termination of the main contract

(1) This declaration of self-commitment is valid until revoked (possible at any time) as long as there is a valid main contract between the parties. With the termination of the main contract, this declaration of self-commitment shall be deemed to be revoked, unless otherwise stated below.

(2) The contractor undertakes to surrender to the principal after termination of the main contract or at any time upon the prinicpal's request all documents, data and data carriers provided to the contractor or - at the principal's request, unless there is an obligation under Union or national law to store the personal data - to delete them. This also applies to any backups made by the contractor. The contractor undertakes to provide documented proof of the proper deletion of any data still in existence.

(3) Upon request, the principal shall be granted the right at any time to check the complete and contractual return or deletion of the data at the contractor in a suitable manner.

(4) The contractor undertakes to treat as confidential any data of which it becomes aware in connection with the main contract, even after the end of the main contract. This declaration of self-commitment shall remain in force after the end of the main contract for as long as the contractor has personal data at its disposal that was sent to it by the principal or which it has collected for the principal.

X. Miscellaneous

(1) The competent supervisory authority is the Austrian Data Protection Authority, Barichgasse 40-42, 1030 Vienna, Austria. The principal and the contractor and, where applicable, their representatives, shall cooperate with the supervisory authority in the performance of their duties upon request.

(2) The following annex is attached to this declaration and forms an integral part thereof:

- **Annex ./1 –** The contractor's technical and organisational measures

1. **Annex ./1 – Technical organisational measures**

Confidentiality

- **Access control**: protection against unauthorised access to data processing systems, e.g.: keys, magnetic or chip cards, electric door openers, porters, security personnel, alarm systems, video systems;
- **Admission control**: protection against unauthorised system use, e.g.: passwords (including corresponding policy), automatic locking mechanisms, two-factor authentication, encryption of data media;
- **Authorisation control**: no unauthorised reading, copying, modification or removal within the system, e.g. standard authorisation profiles on a "need to know" basis, standard process for the allocation of authorisations, logging of accesses, periodic review of the allocated authorisations, especially of administrative user accounts;
- **Pseudonymisation**: if possible for the respective data processing, the primary identifiers of the personal data in the respective data application are removed and kept separately.
- **Classification scheme for data**: due to legal obligations or self-assessment (secret/confidential/internal/public.

Integrity

- **Transfer control**: no unauthorised reading, copying, modification or removal during electronic transmission or transport, e.g.: encryption, Virtual Private Networks (VPN), electronic signature;
- **Input control**: determining whether and by whom personal data has been entered into, changed or removed from data processing systems, e.g.: logging, document management;

Availability and resilience

- **Availability control**: protection against accidental or deliberate destruction or loss, e.g.: backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS, diesel generator), virus protection, firewall, reporting channels and emergency plans; security checks at infrastructure and application level, multi-level backup concept with encrypted outsourcing of backups to an alternative data centre, standard processes in the event of staff changes/departures;

- Rapid **recoverability**;
- **Deletion deadlines**: both for data itself and for metadata such as log files, etc.

Procedures for regular review, assessment and evaluation

- Privacy (data protection) management, including regular staff training;
- Incident Response Management;
- Privacy-friendly default settings;
- **Order control**: no commissioned data processing within the meaning of Art 28 GDPR without corresponding instructions from the principal, e.g.: clear contract design, formalised order management, strict selection of the order processor (ISO certification, ISMS), obligation to convince in advance, follow-up checks.