CONTRACT ON ORDER PROCESSING (ART. 28 para. 3 GDPR)

1. SUBJECT MATTER OF THE AGREEMENT AND ORDER CONTENT

1.1 The subject matter of this Agreement is set out in the agreement concluded between the parties on the provision of software for access via the Internet (SaaS) and/or the purchase of a vehicle scanner between Instavalo GmbH, Gießerallee 23, 47877 Willich, Germany (hereinafter **"Processor"**) and the Client, to which reference is made here (hereinafter **"Main Agreement"**). This Data Processing Agreement (hereinafter the **"Agreement"**) shall apply to all activities related to data processing in the provision of services under the Main Agreement and in which the Processor may come into contact with personal data transmitted or disclosed to the Processor by the Client.

1.2 The type of data processed, the categories of data subjects and the nature and purpose of the collection, processing and use of personal data by the Processor for the Client are set out in detail in **Annex 1** to this Agreement.

1.3 Unless expressly stipulated otherwise in this Agreement, the provision of the contractually agreed data processing shall take place exclusively in Germany, a member state of the European Union (EU) or in another state party to the Agreement on the European Economic Area (EEA). Any transfer to a third country may only take place if the special requirements of Art. 44 et seq. GDPR are met.

2. TECHNICAL AND ORGANIZATIONAL MEASURES

2.1 The Processor must establish security in accordance with Art. 28 para. 3 lit. c, 32 GDPR, in particular in conjunction with Art. 5 para. 1, 2 GDPR. 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 type, 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. The Processor shall document the individual measures in an action plan in **Annex 2**.

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

2.3 The Processor shall regularly monitor the internal processes and the technical and organizational measures to ensure that the processing in its area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the protection of the rights of the data subject is guaranteed.

3. CORRECTION, RESTRICTION AND DELETION OF DATA; RIGHTS OF DATA SUBJECTS

3.1 The Processor may not rectify, erase or restrict the processing of data processed on behalf of the Client without authorization, but only in accordance with documented instructions from the Client. If a data subject contacts the Processor directly in this regard, the Processor shall forward this request to the Client without delay.

3.2 The Processor shall support the Client with suitable technical and organizational measures to ensure the rights of data subjects to be forgotten, rectification, data portability and access. The Processor may claim remuneration for support services that are not owed under the Main Agreement.

4. QUALITY ASSURANCE AND OTHER OBLIGATIONS OF THE PROCESSOR

4.1 When carrying out the work, the Processor shall only use employees who have been bound to confidentiality. The Processor may only process the data in accordance with the Client's instructions, including the powers granted in this Agreement and in the Main Agreement, unless it is legally obliged to do so. The Client shall confirm verbal instructions without delay (at least in text form). The Processor must inform the Client immediately if it is of the opinion that an instruction violates data protection regulations. The Processor is entitled to suspend the implementation of the corresponding instruction until it is confirmed or amended by the Client.

4.2 The Processor shall support the Client in complying with the personal data security obligations set out in Articles 32-36 GDPR, data breach notification obligations, data protection impact assessments and prior consultations. This includes, among other things:

4.2.1 the obligation to report personal data breaches to the Client without delay,

4.2.2 the obligation to support the Client within the scope of his duty to inform the data subjects and to provide the Client with all relevant information in this context without delay,

4.2.3 supporting the Client in its data protection impact assessment.

4.2.4 the support of the Client in the context of prior consultation with the supervisory authority.

4.3 The Processor may claim remuneration for support services that are not included in the service description of the Main Agreement or are attributable to misconduct on the part of the Client.

5. SUBCONTRACTING RELATIONSHIPS

5.1 Subcontracting relationships within the meaning of this provision are those services that are directly related to the provision of the main service. This does not include ancillary services which the Processor uses, for example, as telecommunications services, postal/transport services, maintenance and user service or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the Processor is obliged to make appropriate and legally compliant contractual agreements and to take control measures to ensure data protection and the security of the Client's data, even in the case of outsourced ancillary services.

5.2 The Processor is entitled to engage sub-processors based within the EU or the EEA, provided that it concludes an agreement with the sub-processor in accordance with Art. 28 para. 4 GDPR.

5.3 Subject to the condition set out in Section 5.2, the Client hereby authorizes the Processor to engage the companies listed in **Annex 3** as sub-processors.

5.4 The Processor shall inform the Client in advance of any intended change with regard to the involvement or replacement of other processors. The Client may object to this change vis-à-vis the Processor within 14 days of receipt of the information by the Client. If no objection is made within this period, consent to the change shall be deemed to have been given. An objection may not be made without the interests of the Client outweighing those of the Processor.

6. CONTROL RIGHTS OF THE CLIENT

6.1 The Client shall have the right to carry out inspections in consultation with the Processor or to have them carried out by inspectors to be named in individual cases. The Client shall have the

right to satisfy itself of the Processor's compliance with this Agreement in its business operations by means of spot checks, which must generally be notified in good time.

6.2 The Processor shall ensure that the Client can satisfy itself of the Processor's compliance with its obligations under Art. 28 GDPR. The Processor 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.

6.3 Proof of such measures, which do not only concern the specific order, can be provided by

6.3.1 compliance with approved codes of conduct in accordance with Art. 40 GDPR,

6.3.2 certification in accordance with an approved certification procedure pursuant to Art. 42 GDPR,

6.3.3 Current certificates, reports or report extracts from independent bodies (e.g. auditors, internal audit, data protection officer, IT security department, data protection auditor, quality audit),

6.3.4 suitable certification through an IT security or data protection audit (e.g. in accordance with BSI basic protection or ISO/IEC 27001).

6.4 The Processor may claim remuneration for enabling the Client to carry out inspections.

7. DELETION AND RETURN OF PERSONAL DATA

7.1 Copies or duplicates of the data shall not be created without the knowledge of the Client. Excluded from this are backup copies, insofar as they are necessary to ensure proper data processing, as well as the storage of data that is necessary with regard to compliance with statutory retention obligations.

7.2 After completion of the contractually agreed activities or earlier at the request of the Client - at the latest upon termination of the Main Agreement - the Processor shall hand over to the Client all documents, processing and usage results and data pertaining to the contractual relationship that have come into its possession or, with prior consent, destroy them in accordance with data protection regulations. The deletion log shall be presented upon request. The obligations of the Processor under this Section 7.2 shall not apply if there is an obligation to store the personal data under Union law or the law of the Member States of the EU.

7.3 Documentation that serves as proof of data processing in accordance with the Agreement shall be retained by the Processor beyond the end of the Agreement in accordance with the respective retention periods. The Processor may hand them over to the Client upon termination or expiration of the Agreement in order to discharge the Client.

8. ORDER DURATION, TERMINATION

The term of this Agreement corresponds to the term of the Main Agreement and also includes the period after the end of the Main Agreement until the complete return or deletion of the data provided to the Processor by the Client in connection with the performance of the Main Agreement. The right of either party to terminate this Agreement for good cause remains unaffected.

9. MISCELLANEOUS

9.1 This Agreement shall be governed by German law to the exclusion of the rules of private international law which would lead to the application of a different law.

9.2 The exclusive place of jurisdiction for all disputes arising from or in connection with this Agreement shall be the Processor's registered office. The Processor shall also be entitled to take legal action at the Client's registered office or any other competent court.

9.3 No verbal collateral agreements have been made.

9.4 Should individual provisions of this Agreement be or become invalid in whole or in part, this shall not affect the validity of the remaining provisions. In this case, the parties undertake to replace the invalid provision with a valid provision that comes as close as possible to the economic purpose of the invalid provision. The same applies to any loopholes in the Agreement.

Attachments:

Annex 1: Nature and purpose of the processing, subject matter of the processing, type of data, group of data subjects

Annex 2: Technical and organizational measures

Annex 3: Sub-processors

ANNEX 1 - NATURE AND PURPOSE OF PROCESSING, TYPE OF DATA, CATEGORIES OF DATA SUBJECTS

Data subjects and categories of data subjects	In particular: - Users of the service - Employees of the Client
Type of data or data categories	- Contact details - Data on the use of the software (log data)
Recipients of data	Processors and sub-processors
Nature and purpose of processing	Provision of software for access via the Internet (SaaS); provision of IT services and other services in connection with the software provided and/or the installation and operation of a vehicle scanner, in particular support services

ANNEX 2 - TECHNICAL AND ORGANIZATIONAL MEASURES

The following technical and organizational measures are implemented by the Processor:

1. Confidentiality (Art. 32 para. 1 lit. b GDPR)

a) Access control/building security

Measures to prevent unauthorized persons from gaining access to data processing systems with which personal data is processed and used:

- ☐ Alarm system
- ☐ Video surveillance
- ☐ Automatic access control system, badge reader (magnetic/chip card)
- ☐ Chip cards / transponder systems
- ☐ Light barriers / motion detectors
- ☐ Manual locking system
- ☐ Security locks
- ☐ Key regulation
- ☐ Visitors accompanied by employees
- ☐ Careful selection of cleaning staff
- ☐ Time recording system

b) Access control/security System access

Measures that prevent data processing systems from being used by unauthorized persons:

- ☐ Personal and individual user log-in when logging into the system or company network, including password
- ☐ Authorization process for access authorizations
- ☐ Limitation of authorized users
- ☐ Password procedure (specification of password parameters with regard to complexity and update interval)
- ☐ Managing user authorizations
- ☐ Creating user profiles

- ☐ Single Sign On of the Hüsges One applications
- ☐ Automatic locking of clients after a certain period of time without user activity (also password-protected screen saver or automatic pause)
- ☐ Firewall Sophos
- ☐ Use of intrusion detection systems
- ☐ Use of anti-virus software server
- ☐ Use of anti-virus software clients
- ☐ Use of VPN technology for remote access
- ☐ Encryption of data carriers in notebooks, laptops, etc.

c) Access control/securing access authorizations

Measures that ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage:

- ☐ Use of authorization concepts
- ☐ Number of administrators reduced to the "bare minimum"
- ☐ Management of rights by system administrator
- ☐ Logging of access to applications, in particular when entering, changing and deleting data
- ☐ Password policy incl. password length, password change
- ☐ Authorization process for authorizations
- ☐ File shredder (at least level 3, cross cut)
- ☐ Non-reversible deletion of data carriers

d) Separation control/measures for the separation of data for specific purposes

Measures to ensure that data collected for different purposes can be processed separately:

- ☐ Separation of production and test environment
- ☐ Physical separation (systems/databases/data carriers)
- ☐ Logical multi-client capability of relevant applications
- ☐ Control via authorization concept
- ☐ No productive data in test systems
- ☐ Definition of database rights

e) Pseudonymization and encryption

Measures for pseudonymization and encryption (care must be taken to ensure that the traceability of data to (natural) persons is at least limited):

- ☐ All download/upload connections via the Internet are secured by SSL, SSH or VPN
- ☐ Secure WLAN

2. Integrity (Art. 32 para. 1 lit. b GDPR)

a) Transfer control/security during data transfer

Measures to ensure that personal data cannot necessarily be read, copied, altered or removed during electronic transmission or during their transportation or storage on data carriers and that it is possible to verify and establish to which bodies personal data are intended to be transmitted by data transmission equipment:

- ☐ Installation of dedicated lines or VPN tunnels
- ☐ Encrypted data transmission (https, sftp etc.)
- ☐ Logging of accesses and retrievals

b) Input control/security during data transfer

Measures that ensure that it is possible to subsequently check and determine whether and by whom personal data has been entered, changed or removed in data processing systems:

- ☐ Technical logging of the entry, modification and deletion of data
- ☐ Overview of which applications/programs can be used to enter, change and delete which data
- ☐ Assignment of rights to enter, change and delete data on the basis of an authorization concept
- ☐ Traceability of data entry, modification and deletion through individual user names (not user groups)
- ☐ Clear responsibilities for deletions

3. Availability and resilience (Art. 32 para. 1 lit. b GDPR)

a) Availability control

Measures to ensure that personal data is protected against accidental destruction or loss:

- ☐ Backup & recovery concept
- ☐ Checking the backup process
- ☐ Installing security updates as required
- ☐ Separate partitions for operating systems and data
- ☐ Use of an uninterruptible power supply (UPS)
- ☐ Fire and smoke detection systems
- ☐ Fire extinguisher server room
- ☐ Air-conditioned server room
- ☐ Protective socket strips server room
- ☐ Mirroring hard disks (raid system)
- ☐ No sanitary connections in or above the server room

b) Rapid recoverability (Art. 32 para. 1 lit. c GDPR)

Measures to ensure that deployed systems can be restored in the event of a malfunction and to ensure that all system functions are available and any malfunctions that occur are reported:

- ☐ Recovery according to backup and recovery concept
- ☐ Testing data recovery
- ☐ Sufficient capacity of IT systems and facilities
- ☐ Resilience and error management

4. Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

a) Data protection management

- ☐ The principles of data protection are set out in an internal company policy
- ☐ A data protection officer has been appointed in writing
- ☐ Obligation of employees to maintain data secrecy
- ☐ Obligation of employees to maintain telecommunications secrecy

- ☐ Obligation of employees to maintain social confidentiality
- ☐ The DPO is involved in the data protection impact assessment
- ☐ The DPO is integrated into the organization chart
- ☐ Data protection and data security training for employees
- ☐ A review of the effectiveness of the technical protective measures is carried out regularly
- ☐ The organization complies with the information obligations under Art. 13 and Art. 14 GDPR
- ☐ Formalized process for processing requests for information from data subjects is in place
- ☐ Records of processing activities are kept in accordance with Art. 30 GDPR
- ☐ Regular data protection audits by the data protection officer

b) Incident response management (fault management)

- ☐ Creation of a plan for dealing with disruptions
- ☐ Use of firewall and regular updates
- ☐ Use of spam filters and regular updates
- ☐ Use of virus scanners and regular updates
- ☐ Intrusion Detection System (IDS)
- ☐ Intrusion Prevention System (IPS)
- ☐ Documented process for detecting and reporting security incidents/data breaches (also with regard to the obligation to report to the supervisory authority)
- ☐ Involvement of the data protection officer in security incidents and data breaches

c) Data protection-friendly default settings (Art. 25 para. 2 GDPR) - Privacy by design / Privacy by default

- ☐ Observing privacy by design (data protection) through technology design
- ☐ Compliance with privacy by default through data protection-friendly default settings
- ☐ Selection of data protection-friendly technology during procurement
- ☐ No more personal data is collected than is necessary for the respective purpose
- ☐ Simple exercise of the data subject's right of withdrawal through technical measures

d) Order control

No order processing within the meaning of Art. 28 GDPR without corresponding instructions from the Client

- ☐ Selection of processors with due diligence (in particular with regard to data security)
- ☐ Written documented instructions to the processor
- ☐ Processor has appointed a data protection officer
- ☐ Effective control rights agreed with the processor
- ☐ Prior review and documentation of the security measures taken by the processor
- ☐ Obligation of the processor's employees to maintain confidentiality
- ☐ Ensuring the destruction of data after completion of the order
- ☐ Ongoing review of the processor and its activities

ANNEX 3 – SUB-PROCESSORS

Name of the sub-processor	Address	Description of the services
Webhoster.de AG	Zum Haunert 22 DE-59519 Möhnesee	Server hosting
Sms.at mobile internet services gmbh	Klosterwiesgasse 101b/Ge01 AT-8010 Graz	SMS dispatch
ProfiMasking image processing service	Föhrenstrasse 33 DE-90530 Wendelstein	Image processing
NOEMIX Germany GmbH	Mettlacher Street 5 DE-81379 Munich	Software hosting
DAT - Deutsche Automobil Treuhand GmbH	Helmut-Hirth-Str. 1 DE-73760 Ostfildern	Vehicle data
LOX24 GmbH	Seestr. 109 DE-13353 Berlin	SMS dispatch