Conditions for data processing pursuant to Art. 28 GDPR

[Version: March 2019]

Agreement

between

LexCom Informationssysteme GmbH, Rüdesheimer Str. 23, 80686 Munich, Germany

- hereinafter referred to as the “Contractor” or the “Processor” -

and the users of the ASA Service Quotation Tool (hereinafter referred to as “SQT”)

- hereinafter referred to as the “Controller” –

Note

This document contains the Processor’s conditions for the data processing agreement between the Controller and the Processor pursuant to Art. 28 para. 3 of the General Data Protection Regulation (GDPR). As part of a subsequent declaration to the existing service agreement, the Client agrees to the use of Mitsubishi ASA.

1. Object and duration of the order

(1) Object
The object of the order for data processing is the provision of the Service Quotation Tool (SQT) to existing users of the Mitsubishi ASA spare parts catalogue software.
(2) Duration
The duration of this order (term) corresponds to the term of the Service Agreement.

2. Specification of the content of the order

(1) Nature and purpose of the intended processing of data

In particular, personal data may be processed actively during use of the SQT. Vehicle identification numbers and vehicle registration numbers are processed to determine spare parts. This data may also be evaluated internally by the Contractor as part of created shopping baskets for the purposes of product optimization. Furthermore, end customers' personal/company master data and communication data must be processed in order to submit offers to them using the SQT.
Secondly, personal data may be processed passively by the Contractor (possibility of access as part of maintenance and/or support services). The contractually agreed processing of data will be performed exclusively in a member state of the European Union or in another contracting state to the Agreement on the European Economic Area. Any transfer to a third country requires the prior consent of the Controller and may only take place if the special conditions of Articles 44 et seqq. GDPR are met.

(2) Type of data
The following data types/categories (list/description of the data categories) make up the object of the processing of personal data

- Vehicle identification numbers (VIN) and/or vehicle registration numbers entered by the Controller in the online service

- End customer data entered by the Client in the online service to create offers
    - Personal/company master data
    - Communication data (e.g. telephone, e-mail)

- Personal data saved locally by the Controller (as part of remote maintenance by customer service)
    - Personal/company master data
    - Communication data (e.g. telephone, e-mail)

(3) Categories of data subjects
The categories of data subjects to which the processing relates include:

- End customers of the Controller

3. Technical and organisational measures

(1) The Processor documents the implementation of the required technical and organisational measures set out prior to the award of the contract, in particular with regard to the specific execution of the order, and makes this documentation available to the Controller together with this declaration. Upon acceptance by the Controller, the documented measures become the basis of the order. Otherwise, the parties will not conclude a Service Agreement.

(2) The Processor will ensure the level of security pursuant to Articles. 28 para. 3 lit. c, 32 GDPR in particular in connection with Art. 5 para. 1, para. 2 GDPR. Overall, the measures to be taken are data security measures and measures to ensure a level of protection appropriate to the risk in terms of the confidentiality, integrity, availability and resilience of the systems. In doing so, the Processor shall take into account the state of the art, the implementation costs and the nature, scope and purpose 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 [details in Appendix 1].

(3) The technical and organisational measures are subject to technical progress and further development. In this respect, the Processor is permitted to implement alternative adequate measures. In doing so, it will not fall short of the security level of the specified measures. It must document any major changes.

4. Correction, restriction and deletion of data

(1) The Processor will not correct, delete or restrict the processing of the data to be processed on behalf of the Controller on its own authority. It will only correct, delete or restrict the processing of the data in accordance with the documented instructions of the Controller. Insofar as a data subject contacts the Processor directly in this regard, the Processor will immediately forward this request to the Controller.

(2) Insofar as included in the scope of services, the Processor will immediately ensure a deletion concept, the right to be forgotten, correction, data portability and information in accordance with the Controller's documented instructions. Individual instructions that deviate from the Service Agreement or that present additional requirements, require the prior consent of the Processor. It must be taken into account that the online services provided by the Processor are standard products, the adaptation of which to the Controller’s data protection requirements can result in high costs. These costs are to be paid in full by the Controller in accordance with a corresponding individual agreement.

5. Quality assurance and other duties of the Processor

In addition to complying with the regulations of this order, the Processor also has legal duties in accordance with Articles 28 to 33 GDPR; in particular, it must ensure compliance with the following requirements:

a) Written appointment of a Data Protection Officer, who carries out his duties pursuant to Articles 38 and 39 GDPR. His contact details are communicated to the Controller for the purpose of direct contact. A change of Data Protection Officer will be communicated to the Controller immediately.

b) Safeguarding of confidentiality in accordance with Articles 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 GDPR. When carrying out the work, the Processor will use only employees who have been obliged to maintain confidentiality and who have previously been familiarised with the data protection regulations relevant to them. The Processor and any person reporting to the Processor who has access to personal data, must process such data only in accordance with the instructions of the Controller, including the powers granted in this Contract, unless they are legally obliged to process the data.

c) Implementation and compliance with all technical and organisational measures necessary for this order in accordance with Articles 28 para. 3 sentence 2 lit. c, 32 GDPR [details in Appendix 1].

d) The Controller and the Processor will work together with the supervisory authority on request to fulfil the relevant tasks.

e) Immediate informing of the Controller regarding audit activities and measures by the supervisory authority, insofar as they relate to this order. This also applies if a competent authority investigates the Processor due to an administrative offence or criminal proceedings with regard to the processing of personal data for the commissioned data processing.

f) Insofar as the Controller is subject to an inspection by the supervisory authority, an administrative offence or criminal proceedings, the liability claim of a data subject or a third party or any other claim in connection with the data processing by the Processor, the Processor will support the Controller to the best of its ability.

g) The Processor will regularly review the internal processes and technical and organisational measures to ensure that the processing within its area of responsibility complies with the requirements of applicable data protection law and ensures the protection of the data subject's rights.

h) Verifiability vis-à-vis the Controller of the technical and organisational measures taken within its supervisory powers in accordance with Section 7 of this Contract.

6. Subcontractual relations

(1) For the purposes of this regulation, subcontractual relationships are those services that relate directly to the provision of the main service. This does not include ancillary services provided by the Processor e.g. telecommunication services, postal/transport services, maintenance and user services or the disposal of data storage devices as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software for data processing systems. However, even in the case of outsourced ancillary services, the Processor is obliged to take appropriate and legally compliant contractual agreements and control measures to ensure the protection and security of the Controller's data.

(2) The Processor will commission subProcessors (other data processing companies) only with the prior explicit written or documented consent of the Controller.
The Controller agrees to the commissioning of the following subcontractor under the condition of a contractual agreement in accordance with Art. 28 para. 2–4 GDPR:

Subcontractor’s company	Address/country	Service
Belenus LOB GmbH	Rüdesheimer Str. 23 80686 Munich Germany	Provision of entire internal and external IT operations

The current subcontractor can be changed provided:

- The Processor notifies the Controller of such outsourcing to a subcontractor a reasonable time in advance in writing or in text form and
- The Controller does not object to the planned outsourcing in writing or in text form by the time the data is passed over to the Processor and
- A contractual agreement or binding declaration in accordance with Art. 28 para. 2-4 GDPR is taken as the basis.

(3) The transfer of the Controller's personal data to the subcontractor and its commencing work are only permitted if all conditions for subcontracting are met.

(4) Any further outsourcing by the subcontractor requires the express consent of the Processor (in text form as a minimum); all contractual regulations in the contracting chain must also be imposed on the additional subcontractor.

7. Monitoring rights of the Controller

(1) In consultation with the Processor, the Controller is entitled to carry out inspections or have them carried out by auditors who are to be named in individual cases. It is entitled to carry out spot checks to verify that the Processor is in compliance with this Agreement in its business operations. The Controller must notify the Processor in good time that it intends to conduct such a spot check. Such spot checks must be carried out during normal business hours without disturbing the Processor’s course of operations, while maintaining strict confidentiality with regard to the Processor's operating and business secrets.

(2) The Processor will make sure that the Controller can satisfy itself of the compliance with the duties of the Processor in accordance with Art. 28 GDPR. The Processor undertakes to provide the Controller with the necessary information upon request and, in particular, to provide evidence of the

implementation of the technical and organisational measures. As a rule, the Controller can carry out one inspection per calendar year; additional checks are permitted in the case of specific incidents.

(3) The Processor is entitled, at its sole discretion and taking into account the statutory obligations of the Controller, not to disclose information that is sensitive with regard to the Processor's business or if the Processor would breach any legal or contractual obligations by disclosing such information.

(4) At the Processor’s discretion, the proof of such measures that relate not only to the specific order can be made by the following means instead of an on-site inspection

a) Compliance with approved codes of conduct pursuant to Art. 40 GDPR
b) Certification in accordance with an approved certification mechanism pursuant to Art. 42 GDPR
c) Current attestations, reports or excerpts of reports from independent entities (e.g. auditors, review, Data Protection Officer, IT security department, data protection auditors, quality auditors)
d) Appropriate certification from an IT security audit or data protection audit (e.g. in accordance with the baseline security of the German Federal Office for Information Security (BSI)).

A prerequisite for this is that this measure enables the Controller to reasonably satisfy itself of the compliance with the technical and organisational measures as specified in the Appendix to this Agreement.

(5) The Processor may assert a claim for compensation for enabling the Controller to perform checks.

8. Notification in case of violations on the part of the Processor

(1) The Processor shall assist the Controller in complying with the obligations relating to the security of personal data, reporting of data breaches, data protection impact assessments and prior consultations, as set out in Articles 32 to 36 GDPR. This includes but is not limited to:

a) Ensuring an adequate level of protection through technical and organisational measures that take into account the circumstances and purposes of the processing and the predicted likelihood and severity of a possible breach of rights due to security vulnerabilities, and enable the immediate detection of relevant violation events
b) The duty to report personal data breaches to the Controller without delay
c) The obligation to support the Controller in its duty to provide information to the data subject and to provide it with all relevant information in this context without delay
d) Providing assistance to the Controller for its data protection impact assessment
e) Supporting the Controller in the context of prior consultations with the supervisory authorities

(2) The Processor may claim reasonable compensation for provision of support that is not included in the Service Agreement or is not the result of misconduct by the Processor.

9. Authority of the Controller

(1) The Controller shall confirm verbal instructions immediately (in text form as a minimum).

(2) The Processor will inform the Controller immediately if it believes that an instruction violates data protection regulations. The Processor is entitled to suspend the execution of the relevant instruction until it is confirmed or amended by the Controller. The Processor may assert a claim for compensation against the Controller for expenses that it incurs as a result of this.

10. Deletion and return of personal data

(1) Copies or duplicates of the data will not be created without the knowledge of the Controller. This does not include backup copies, to the extent that these are necessary to ensure proper data processing, and data that is required for compliance with statutory retention requirements.

(2) Upon completion of the contractually agreed work or earlier at the request of the Controller – at the latest upon termination of the Service Agreement – the Processor must hand over to the Controller all documents that have come into its possession, results of processing and utilisation as well as datasets created in connection with the contractual relationship or, with prior consent, destroy them in line with data protection guidelines. The same applies to test material and discarded material. The log documenting the deletion must be submitted on request.

(3) The Processor will retain documentation that serves to provide evidence of the proper data processing as per the order beyond the end of the Contract in accordance with the respective retention periods. It can hand this documentation over to the Controller at the end of the contract term.

Appendix – Technical and organisational measures

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

- Building entry control
  No unauthorised access to data processing systems, e.g.: magnetic or chip cards, keys, electric strikes, security personnel or gatekeepers, alarm systems, CCTV
- System access control
  No unauthorised use of systems, e.g.: (secure) passwords, automatic locking mechanisms, two-factor authentication, encryption of data storage devices
- Data access control
  No unauthorised reading, copying, modification or removal within the system, e.g.: authorisation concepts and needs-based access rights, logging of all access
- Separation control
  Separate processing of data collected for different purposes, e.g. multi-client capability, sandboxing

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

- Disclosure control
  No unauthorised reading, copying, modification or removal during electronic transfer or transport, e.g.: encryption, virtual private networks (VPN), electronic signature.
- Entry control
  Specification of whether and by whom personal data has been entered or modified in or removed from data processing systems, e.g.: logging, document management.

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

- Availability control
  Protection against accidental or wilful destruction or loss, e.g.: backup strategy (online/offline, on-site/off-site), uninterruptible power supply (UPS), virus protection, firewall, reporting channels and emergency plans.
- Ability to restore the availability and access to personal data in a timely manner (Art. 32 para. 1 lit. c GDPR);

4. Process for regular monitoring, assessment and evaluation

(Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

- Data protection management
- Incident response management
- Privacy by default settings (Art. 25 para. 2 GDPR);
- Order control
  No commissioned data processing within the meaning of Art. 28 GDPR without corresponding instructions from the Controller, e.g.: clear contract design, formalised order management, strict selection of the service provider, duty to satisfy in advance, follow-up checks