Commissioned data processing in accordance with Article 28 of the General Data Protection Regulation (*Datenschutz-Grundverordnung*, DSGVO)

between

hereinafter referred to as Principal,

and

active logistics AG, Gahlenfeldstraße 53, 58313 Herdecke

and the subsidiary companies

active logistics Herdecke GmbH, Gahlenfeldstr. 53, 58313 Herdecke

active logistics Koblenz GmbH, Bahnhofplatz 9, 56068 Koblenz

active logistics AG, Kundenzentrum Niederaula, Industriestraße 5, 36272 Niederaula

active logistics Nürnberg AG, Lina-Ammon-Straße 22, 90471 Nürnberg

hereinafter referred to as Processor,

and hereinafter referred to jointly as 'Contracting Parties' and individually as 'Contracting Party'.

Table of contents

0 Recitals

This Agreement ascertains the obligations of the Contracting Parties under data protection law which arise from the main contract for the commissioned data processing described in detail. It shall apply to all work related to the main contract and to the personal data of the Principal which the Processor's employees or third parties commissioned by the processor of the order could come into contact with. The contractual term of this annex is determined by the term of the main contract.

This Agreement takes into account the currently prevailing norms in the applicable EU General Data Protection Regulation and the German Federal Data Protection Act (*Bundesdatenschutzgesetz*), which was passed by both houses of the German parliament on 27 April 2017 (*Bundestag*) and on 12 May 2017 (*Bundesrat*).

1 Definitions

<u>According to General Data Protection Regulation</u>

(1) Personal data (see 'Definitions' in Article 4 no. 1 of the General Data Protection Regulation)

'Personal data' is any information relating to an identified or an identifiable natural person (hereinafter referred to as 'Person Affected');

(2) Processor (see 'Processor' in Article 28 of the General Data Protection Regulation)

The 'Processor' is a natural or legal person, government authority, or another entity that processes personal data on behalf of the entity or person responsible for the data.

(3) Instructions (see 'Processor' Article 28 no. 3 a) of the General Data Protection Regulation)

The processor processes the personal data only according to the documented instructions of the entity or person responsible – also with respect to transferring personal data to a third country or an international organisation.

2 Subject-matter and term of the order

2.1 Subject-matter of the order

The Processor processes data on behalf of the Principal which arises from the main contract/service agreement.

2.2 Term of the order

The time period of the order (term) is determined by the main contract.

3 Specification of the contents of the order

3.1 Scope, type and purpose of the designated collection, processing or use of data

(1) The type and purpose of processing personal data by the Processor for the Principal is described in detail in the service agreement.

(2) Performance of the data processing contractually agreed upon is carried out exclusively in a member state of the European Union or in another contracting state of the Treaty on the European Economic Area. Any relocation to a third country requires the prior approval of the Principal and may only be carried out if the special requirements set out in sections 4b and 4c of the German Federal Data Protection Act and Article 44 et seq. of the General Data Protection Regulation are met.

3.2 Type of Data

The subject-matter of the personal data processing is described in ***[Annex 1]*** in section 1 'Type of data'.

3.3 Categories of the persons affected

The categories of the persons affected by the processing are described in ***[Annex 1]*** in section 2 'Categories of the persons affected'.

4 Technical and organisational measures

(1) The Processor shall explain to the Principal for it to review how the technical and organisational measures described prior to the contract being awarded will be implemented before beginning the processing, especially with respect to the execution of the contract. In the event the Principal accepts these measures, the documented measures shall be the basis for the order. If the Principal's review/audit results in adjustments needing to be made, they must be implemented by mutual agreement. The Principal shall bear any costs.

(2) The Processor shall take into account the security requirements set out in to Article 28 no. 3 letter c) and Article 32 of the General Data Protection Regulation, in particular in conjunction with Article 5, paragraphs 1 and 2 of the General Data Protection Regulation. In general, the measures to be taken into account concern data security measures and ensuring a suitable level of protection for the risk in terms of confidentiality, integrity, availability and resilience of the systems. For this purpose, the state-of-the art technology and the implementation costs as well as the type, scope and purpose of the processing must be taken into account in addition to the different probability of occurrence and the level of risk of infringing upon the rights and freedoms of natural persons as defined in Article 32, paragraph 1 of the General Data Protection Regulation ***[details presented in Annex 5]***.

(3) The technical and organisational measures are subject to technical advancements and further development. In this respect, the Processor is authorised to implement alternative adequate measures. In doing so, the level of security of the pre-defined measures may not fall excessively short. Any significant modifications must be documented. The Processor shall inform the Principal of any major changes.

5 Amending, restricting and deleting data

(1) The Processor is not permitted to arbitrarily amend the data being processed and instead must amend, delete or block data or restrict its processing according to the Principal's documented instructions. If a person affected contacts the Processor directly about this, the Processor shall forward the request to the Principal.

(2) If it is part of the scope of services being provided, the Processor must ensure that the deletion policy, right to be forgotten, corrections, data portability and information are carried out according to the Principal's documented instructions.

6 Quality assurance and other duties of the Processor

In addition to complying with the rules in this contract, the Processor must also comply with legal obligations under Articles 28 to 33 of the General Data Protection Regulation; in this respect, the Processor shall ensure compliance with the following guidelines in particular:

- Orders in writing, provided they are legally required and a data protection officer who can perform his/her duty in accordance with Article 38 and 39 General Data Protection Regulation in conjunction with section 38 of the German Federal Data Protection Act (new version). The contact information of the Processor's data protection officer is:

  Stefan Kleinermann +49 (0) 2401 60 540 info@das-datenschutz-team.de

  For the data center Niederaula:

  DPP Data Protection GmbH +49 (0) 69175366960 rf@dataprotectionpartner.de

- The contact information of the Principal's data protection officer is described in the 'Contact information at the Principal' section in ***[Annex 4]***.

  If a new data protection officer is named, the other respective party must be informed without delay.

- Maintaining confidentiality must be carried out according to Article 28 paragraph 3 sentence 2 letter b), Articles 29 and 32, paragraph 4 of the General Data Protection Regulation. When carrying out the work, the Processor shall only use employees who are required to maintain confidentiality and who have previously become familiar with the relevant provisions pertaining to data privacy. The Processor and any person under its authority who has access to personal data may only process this data according to the Principal's instructions and the powers conferred in this Contract, unless they are legally required to process the data.
- The implementation and compliance with all of the technical and organisational measures required for this Contract shall be carried out according to Article 28, paragraph 3, page 2, letter c) and Article 32 of the General Data Protection Regulation ***[details provided in Annex 5]***.
- Upon request, the Principal and the Processor shall work together with the regulatory authority when performing their tasks.
- Information about auditing activities and measures being taken by the regulatory authorities must be disclosed immediately with the Principal provided they relate to this Contract. This shall also apply if a competent authority is investigating a regulatory or criminal offence with respect to processing personal data during processing at the Processor's company.
- The Processor must support the Principal to the best of its ability if the Principal is subject to inspection by the regulatory authorities, if regulatory or criminal proceedings are pending, if the person affected has asserted a liability claim, or if another claim related to order processing at the Processor's company has been made.
- The Processor controls the internal processes as well as the technical and organisational measures in order to guarantee that the processing under its scope of responsibility is carried out in accordance with the requirements of

applicable data protection laws and that the rights of the persons affected are protected.

- The technical and organisational measures that are implemented must be traceable for the Principal as it falls within the scope of its power to monitor in accordance with section 9 of this Contract.

7 Sub-contractual relations

(1) Sub-contractual relations as defined in this provision are to be understood as services which relate directly to the main service being provided. This does not include ancillary services which the Processor uses such as telecommunication services, mail/transport services, maintenance and user services, the disposal of data media or any other measures taken to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. The Processor is, however, obligated to safeguard data privacy and the data security of the Principal's data and to make suitable contractual arrangements that are compliant with the law; this shall also apply in the event ancillary services are outsourced.

(2) The Processor is only allowed to commission subcontractors (other processors) at any time if

- The Processor has notified the Principal of the said outsourcing to a subcontractor in writing or in text form and has given the Principal a reasonable period of advance notice and

- The Principal has not informed the Processor of its objection to the planned outsourcing in writing or in text form before the point in time when the data is to be transferred and

- It is based on a contractual agreement which complies with Article 28 para. 2-4 of the General Data Protection Regulation.

- The subcontractors commissioned by the Processor are described in the 'Directory of subcontractors' section in ***[Annex 2]***.

8 The Principal's control rights and other duties

(1) The Principal has the right to carry out checks during normal work hours in coordination with the Processor, or in exceptional cases, to have these checks carried out by designated inspectors. The Principal has the right to make sure that the Processor is complying with this agreement by means of making spot checks of his business operations during normal work hours, which must be announced in a timely manner. The Principal shall ensure that the checks are only carried out in the scope required so that the Processor's business operations are not disrupted excessively.

(2) The Processor shall ensure that the Principal can make sure that the Processor's duties are being met in accordance with Article 28 of the General Data Protection Regulation. The Processor is obligated to provide the Principal with the necessary information upon request and in particular to show evidence that the technical and organisational measures have been implemented.

(3) The Processor can provide proof of these types of measures that relates to the specific order by

- Complying with the approved rules of conduct under Article 40 of the General Data Protection Regulation;
- Obtaining certification according to an approved certification procedure under Article 42 of the General Data Protection Regulation;
- Submitting current attestations, reports or reports extracted from independent review bodies (e.g. auditors, reviewers, data protection officers, IT security department, data protection auditors and quality assurance auditors);
- Obtaining appropriate certification from an IT security or data protection audit (for example according to the 'BSI-Grundschutz' manual published by the German Federal Office for Information Security).

(4) The Processor can assert a claim for remuneration in order to make it possible for the Principal to carry out inspections.

9 Notification in the event of violations by the Processor

(1) The Processor shall support the Principal in complying with the duties indicated in Articles 32 to 36 of the General Data Protection Regulation which pertain to the security of personal data, reporting data breaches, making data protection impact assessments and conducting prior consultations. This includes, among other things:

a) Safeguarding a suitable level of protection by taking technical and organisational measures that take into account the circumstances and aims of the processing as well as the projected probability and seriousness of a possible infringement of rights by gaps in security and that make it possible to immediately ascertain relevant incidents of breaches

b) The duty to report breaches of personal data to the Principal

c) The duty to support the Principal while fulfilling its reporting obligation to the individuals affected and to provide the Principal all relevant information related thereto
d) Supporting the Principal with his data protection impact assessment
e) Assisting the Principal with the regulatory authorities during prior consultations

(2) The Processor can charge fees for providing assistance services that are not included in the performance specification or which are not attributable to failures on the part of the Processor.

10 The principal's authority to direct

(1) The Principal shall confirm verbal instructions without delay (the minimum requirement is text form).

(2) The Processor must inform the Principal immediately if it is of the opinion that one of the instructions violates data protection regulations. The Processor is authorised to suspend its performance until the respective instruction has been confirmed or changed by the Principal.

(3) Before beginning the processing of the data in the order, both parties shall designate the Principal's employees who are authorised to issue instructions as well as the Processor's employees who are authorised to receive instructions in writing; see 'Directory of people responsible' in ***[Annex 4]***. If a new contact person has been assigned or the contact person is hindered from performing his/her duties, the contractual partner must inform the other party of the replacement or proxy in writing.

11 Duties to maintain confidentiality

(1) Both parties are obligated to treat all information which they receive concerning the execution of this Contract confidentially for an unlimited period of time and only to use this information for the execution of this Contract. No party is entitled to use this information either partially or in its entirety for any purpose other than the previously mentioned purposes or to make this information available to a third party.

(2) The aforementioned duty shall not apply to information which a party verifiably has received by a third party without having obligated itself to maintain confidentiality or which it became aware of through public knowledge.

12 Deletion and return of personal data

(1) Copies or duplicates of the data that fall outside the scope of the commissioned work shall not be made without the Principal's knowledge. Exceptions to this rule are backup copies, provided they are required for ensuring proper data processing, as

well as copies of data which are required for complying with legal obligations to retain data.

(2) The Processor must give the Principal all documents in its possession, its processing and utilization results and the data files related to the contractual relations after the contractually agreed work is completed or when the Principal requests beforehand – at the latest upon the completion of the service agreement. Alternatively the Processor can destroy such materials according to data protection requirements upon receiving the Principal's prior consent. The same policy shall apply to testing and rejected materials. The deletion records must be submitted when requested.

(3) Documentation which serves to prove that data processing was carried out properly and as ordered must be kept by the Processor according to the respective record retention periods after the contract ends. To ease the Processor's burden, the Processor can give these documents to the Principal at the end of the contract.

13 Final provisions

(1) Should the Principal's property be endangered by the Processor as a result of measures being taken by a third party (such as by garnishment or seizures), or by insolvency proceedings or through any other events, the Processor must inform the Principal. The Processor shall inform creditors about the fact that the matter concerns data which is being processed on the Principal's behalf.

(2) Any additional agreements must be made in written form.

(3) German law shall apply.

(4) If individual sections of this Contract are invalid, this shall not affect the validity of the remaining provisions in this Contract.

Town/City, date .....

.....
Principal

Town/City, date .....

.....
Processor

Annex 1

I. Description of the data and the people affected

1. Type of data

The subject matter of the personal data processing is the following types of data and data categories (list/description of data categories);

Customer master data *(e.g. first and last name, address, business partner's number, contract account number and customer history)*
Supplier master data *(e.g. first and last name, address and the contact person's position)*
Business partner or contact person's data *(e.g. first and last name, address and the contact person's position)*
Communication data *(e.g. email, telephone and fax number)*
Customer's billing and payment information *(e.g. consumption information, bank account information, payment/late payment history, credit rating information)*
Suppliers' billing and payment information *(e.g. bank account information, payment/late payment history, credit rating information)*
Recording-keeping data *(e.g. user ID, IP address if applicable, log-in and modification history and data records)*

2. Categories of the people affected

The categories of the persons affected by the processing include:

Employees
Interested parties
Customers
Suppliers
The customer's or supplier's employees (contact persons)
Business partners

Annex 2

II. Directory of subcontractors

Subcontractor	Place of business	Service provided
Vision-Flow Software GmbH	Riedgasse 11, A – 6850 Dornbirn	Programming
IMC Zlin a.s.	Kvitkovà 119, CZ 76001 Zlin	Programming
Prologia Unternehmensberatung GmbH	Dietigheimer Str. 18, 61350 Bad Homburg	Programming

Annex 3

III. Directory of the persons responsible

In particular, the Principal designates the following contact persons as **authorised to give instructions** to the Processor:

Mr/Ms:
Tel.:
Mobile:
Email:

and

Mr/Ms:
Tel.:
Mobile:
Email:

In particular, the Processor designates the following contact persons as **authorised to receive instructions** from the Principal:

Mr/Ms:
Tel.:
Mobile:
Email:

and

Mr/Ms:
Tel.:
Mobile:
Email:

Annex 4

IV. Contact information of the Principal's data protection officer

The following person is appointed as the data protection officer at the Principal's company:

Mr/Ms:
Tel.:
Mobile:
Email:

Annex 5

V. The Processor's technical and organisational measures in accordance with Article 32 of the General Data Protection Regulation

1. Confidentiality (Article 32, paragraph 1, b) of the General Data Protection Regulation)

Entry control *(No unauthorised access to data processing systems and filing locations of the information (e.g. magnet or chip cards, keys, electrical door opener, facility security, doorman, alarm systems, video surveillance systems, offices)*	Access control system, card reader, chip card
	Recording assignments or keys
	Door locking device (electrical door)
	Reception/gate
	Monitoring systems, e.g. alarm system, video/TV monitor
	Locking systems
Access control *(No unauthorised use of systems, e.g. (secure) passwords, automatic blocking mechanisms, two-factor authentication, encryption of data media)*	Password procedure (special characters, minimum length of 8 characters, changing the password on a regular basis)
	Automatic locking of terminal devices when inactive/screen lock
	Setting up one user master record per user
	Encrypting mobile storage devices
	Domain log-in
Access control *(Needs-oriented design of a policy for amending data and access rights as well as their monitoring and record-keeping: no unauthorised viewing, copying, changing or removing information within the system, e.g. policies for amending data and needs-based access rights as well as record-keeping of everyone who has had access)*	Differentiated authorisations (profiles, personas, transactions and objects)
	Regular assessments and reviews of existing authorisations
	Prompt updates and cancellation of authorisations
	Encryption of data requiring special protection
	Access to customer systems via VPN or ISDN dial-in using RDP, SSH, TeamViewer, PCVisit or Telnet
	Router authentication using an encrypted identifier and password
	Monitoring remote maintenance

Separation control *(Measures for separate processing (saving, changing, deleting, transferring) data for different purposes. Separate processing of data which was collected for different purposes, e.g. multi-client capability, sandboxing)*	Internal multi-client capability/ earmarking
	Separation of functions (production/ test/development), to the extent possible
	Pseudonymisation (Article 32, para 1, a) and Article 25 para 1 of the General Data Protection Regulation) in testing and/or development systems

2. Integrity (Article 32, paragraph 1, letter b) of the General Data Protection Regulation)

Transfer control *(No unauthorised viewing, copying, changing or deletion during electronic transmission or transport, e.g. encryption, Virtual Private Networks (VPN), electronic signature)*	Encryption/tunnel connection (VPN) or ISDN direct dial-in
	Electronic signature
	Record-keeping
	Transport security
Entry control *(Determining if data was entered into the data processing systems and by whom and if it was changed or removed e.g.: record-keeping and document management)*	Record-keeping and auditing systems
	Record-keeping of database access through alH.4

3. Availability and resilience (Art. 32, para 1, letter b) of the General Data Protection Regulation)

Availability control *(Protection from accidental or deliberate destruction or loss, e.g. a backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), virus protection, firewall, reporting channels and emergency/contingency plans)*	Backup Process (responsibility of the Principal)
	Mirroring hard disks, e.g. RAID Process
	Uninterruptible power supply (UPS)
	Separate storage of backup media
	Virus protection/firewall
	Emergency/contingency plans
	Fast recoverability (Art. 32, para 1, letter c) of the General Data Protection Regulation)

4. Procedure for regular audits, assessment and evaluation (Art. 32, para 1 letter d) and Art. 25, para 1 of the General Data Protection Regulation)

Data protection management	Data Protection by technology design (privacy by design, Art. 25 paragraph 1 of the General Data Protection Regulation)
	Data-protection-friendly default settings (privacy by default, Art. 25, paragraph 2 of the General Data Protection Regulation)
Incident management	Incident management (1st level, 2nd level)
Order control *(No commissioned data processing as defined in Art. 28 of the General Data Protection Regulation without the Principal's corresponding instructions, e.g. clear contract design, formalised order management, strict selection of service provider, duty to be satisfied ahead of time, follow-up checks)*	Only the individuals authorised to give the Principal's instructions can issue instructions.
	Only instructions issued in writing
	Formalised order placement (order form)
	Clear contract design
	Criteria for selecting an agent if a subcontractor is used
	Monitoring the execution of the contract if subcontractors are used