ORdER PROCESSING AGREEMENT

[Order Processing Agreement pursuant to Art. 28 GDPR]

RESPONSIbLE PARTY

Company XYZ /
John Smith

Street name, 1234 City name
Country name

(hereinafter referred to as the Principal)

ORdER PROCESSOR

ESA Elektronische Steuerungs- und Automatisierungs Ges.m.b.H.

Steyrer Straße 6A, 4493 Wolfern
(hereinafter referred to as the Contractor)

1. PREAMBLE

The Principal uses ESA software products such as ESAweight, ESAprocess, ESAlogistic process control systems and their modules. They are put into operation, serviced and maintained by ESA. The systems run on operating systems whose installation and maintenance are at least partially carried out by the Contractor.
This Agreement shall be understood as either an addition to any existing license, service or maintenance contracts, or as a separate Agreement if no service/maintenance contract has been entered into (yet).

2. SUBJECT OF THE AGREEMENT

2.1. The subject of this contract is the execution of the following tasks, which require an agreement on the personal data provided by the Principal: Commissioning, support, maintenance and updates of ESA software products, such as process control systems ESAweight, ESAprocess, ESAlogistic and their modules, or remote maintenance in the IT environment via Team Viewer or RDP (Remote Desktop Connection)

2.2. The following data categories are processed: order data, item data, recipe data, customer and supplier data, process data

2.3. The following categories of involved persons are subject to processing: customers, suppliers, contact persons, employees, etc.

3. DURATION OF THE AGREEMENT

3.1. The agreement ends with the termination of an existing service or maintenance contract. The chance of extraordinary termination for good cause shall remain unaffected.

3.2. If there is no service or maintenance contract, the Agreement is concluded for an indefinite period of time and can be terminated by both parties at any time.

4. OBLIGATIONS OF THE CONTRACTOR

4.1. The Contractor undertakes to process data and processing results solely within the scope of the Principal's written orders. If the Contractor receives an official order to make the Principal’s data available, the former shall - insofar as legally permissible - inform the latter without delay, and report this to the authorities. Similarly, processing the data for the Contractor’s own purposes requires a written order.

4.2. The Contractor declares in a legally binding manner to have obliged all the persons in charge of data processing to confidentiality prior to beginning the activity, or to have informed them that they are subject to an appropriate statutory duty of confidentiality. In particular, the obligation of confidentiality of the persons in charge of data processing shall remain valid even after the termination of their duties and the end of their collaboration with the Contractor.

4.3. The Contractor declares in a legally binding manner to have taken all necessary measures to ensure the security of processing pursuant to Art. 32 GDPR (details can be found in Annex ./1).

4.4. The Contractor shall take technical and organisational measures so that the Principal can fulfil the data subject’s rights in accordance with Chapter III of the GDPR at any time (information, rectification and deletion, data portability, opposition, and automated decision-making on a case-by-case basis) within the statutory periods, providing the Principal with all necessary information for this purpose. If a request is made to the Contractor in which it turns out that the Applicant mistakenly considers the Contractor to be the Principal with regards to the data application, the Contractor shall immediately forward the request to the Principal and notify the Applicant.

4.5. The Contractor shall assist the Principal in complying with the obligations set out in Articles 32 to 36 GDPR (data security measures, personal data breach notifications to the supervisory authority, notification of the person affected by a personal data protection infringement, privacy impact assessment, prior consultation).

4.6. The Contractor is advised that, for this order processing, they are required to create a record of processing activities pursuant to Art. 30 GDPR.

4.7. With regards to the processing of the data provided by the Principal, the latter is granted the right to inspect and control the data processing facilities, even through third parties commissioned by them, at any time. The Contractor undertakes to provide the Principal with all information necessary to check for compliance with the obligations set out in this Agreement.

4.8. Upon termination of this Agreement, the Contractor undertakes to destroy on behalf of the Principal all processing results and documentation containing data. If the Contractor processes data in a special technical format, the latter undertakes, after the termination of this Agreement, to make data available either in this format or, upon the Principal's request, in the format in which the Contractor received the data from the Principal, or in another common format..

4.9. The Contractor shall inform the Principal immediately if they believe that an instruction of the Principal violates the data protection regulations of the European Union or of the member states.

5. PLACE OF EXECUTION OF DATA PROCESSING

All data processing activities are carried out exclusively within the EU/EEA.

6. SUB-PROCESSORS

The Contractor may subcontract IT services as well as software development, consulting, etc. to sub-processors. The Contractor shall enter into the required agreements, pursuant to Art. 28 (4) GDPR, with the Sub-processor. In doing so, it shall be ensured that the Sub-processor undertakes the same obligations as the Contractor under this agreement. If the Sub-processor fails to comply with its data protection obligations, the Contractor shall be held liable for compliance with the Sub-processor's obligations by the Principal.

7. MISCELLANEOUS

Any changes or additions to this Agreement must be made in writing. Should a contractual provision be or become ineffective or void, this shall not affect the validity of the remaining provisions. On the contrary, the contracting parties undertake to replace the ineffective or void provision with an effective provision which is as similar as possible in the economic purpose to be achieved. All disputes arising from or in connection with this Agreement shall be governed by Austrian law.

COMPANY XY / JOHN SMITH

Function/Stamp/DD.MM.YYYY

PRINCIPAL	CONTRACTOR – ESA GMBH
[NAME IN CAPITAL LETTERS/ FUNCTION/DATE/SIGNATURE]	[NAME IN CAPITAL LETTERS/ FUNCTION/DATE/SIGNATURE]

ANNEX 1

TECHNICAL AND ORGANISATIONAL MEASURES

CONFIDENTIALITY

Data access control: Protection against unauthorised access to data processing systems, e.g.: Keys, magnetic stripe or chip cards, electric door openers, porters, security guards, alarm systems, video installations;
Admission control: Protection against unauthorised use of the system, e.g.: Passwords (including relevant policy), automatic locking mechanisms, two-factor authentication, disk encryption;
System access 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 authorisation assignment, access logging, periodic checking of assigned authorisations in particular of administrative user accounts;
Pseudonymisation: If possible for the relevant data processing, the primary identification features of personal data in the relevant data application shall be removed and stored separately.
Data classification scheme: Due to legal obligations or self-assessment (secret/confidential/internal/public).

INTEGRITY

Dissemination control: No unauthorised reading, copying, modification or removal during electronic transmission or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature;
Entry control: Determining if and by whom personal data has been entered, changed or removed in data processing systems, e.g.: Logging, document management

AVAILABILITY AND RESILIENCE

Availability control: Protection against accidental or wilful destruction or loss, e.g.: Backup strategy (online/offline, on-site/off-site), uninterruptible power supply (UPS, diesel generator set), antivirus, firewall, messaging options and emergency plans; security checks at infrastructure and application levels, multi-level security concept with encrypted outsourcing of backups to an alternative data centre, standard processes for employee turnover/resignations;

Rapid recoverability;

Deletion time: Both for data itself and metadata such as logfiles, etc.

PROCEDURES FOR REGULAR REVIEW, ASSESSMENT AND EVALUATION

Data protection management, including regular employee training;
Incident response management;
Order control: No order data processing pursuant to Art. 28 GDPR without appropriate instructions from the Principal, e.g.: clear contract drafting, formalized order management, strict selection of the order processor (ISO certification, ISMS), vetting duty, follow-up checks.