DER VERANTWORTLICHE

Musterfirma / Max Mustermann

Musterstraße 1, 1234 Musterort

(im Folgenden Auftraggeber)

DER AUFTRAGSVERARBEITENDE

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

Steyrer Straße 6A, 4493 Wolfern

(im Folgenden Auftragnehmer)

1. PRÄAMBEL

Der Auftraggeber hat Softwareprodukte von ESA im Einsatz, wie Prozessleitsysteme ESAweight, ESAprocess, ESAlogistic und deren Module. Diese werden durch die Fa. ESA in Betrieb genommen, serviciert und gewartet. Die Systeme laufen auf Betriebssystemen, deren Installation und Wartung zumindest teilweise durch den Auftragnehmer erfolgt.

Diese Vereinbarung ist entweder als Ergänzung zu bestehenden Lizenz-, Services und Wartungsverträgen zu verstehen bzw. als eigenständige Vereinbarung, wenn (noch) kein Service/Wartungsvertrag besteht.

2. GEGENSTAND DER VEREINBARUNG

2.1. Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben, die eine Vereinbarung von personenbezogenen Daten, die vom Auftraggeber überlassen wurden, erfordert: Inbetriebnahme, Support, Wartung und Updates der ESA Softwareprodukte, wie Prozessleitsysteme ESAweight, ESAprocess, ESAlogistic und deren Module, oder der IT-Umgebung per Fernwartung via Team Viewer oder RDP (Remotedesktopverbindung)

2.2. Folgende Datenkategorien werden verarbeitet: Auftragsdaten, Artikeldaten, Rezeptdaten, Kunden und Lieferantendaten, Vorgangsdaten

2.3. Folgende Kategorien betroffener Personen werden unterliegen der Verarbeitung: Kunden, Lieferanten, Ansprechpartner, Beschäftigte, udg.

3. DAUER DER VEREINBARUNG

3.1. Die Vereinbarung endet mit der Beendigung eines vorhandenen Service bzw. Wartungsvertrages. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3.2. Besteht kein Service bzw. Wartungsvertrages, ist die Vereinbarung auf unbestimmte Zeit geschlossen und kann von beiden Parteien jederzeit gekündigt werden.

4. PFLICHTEN DES AUFTRAGNEHMERS

4.1. Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

4.2. Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

4.3. Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage „Technisch organisatorische Maßnahmen“ zu entnehmen).

4.4. Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

4.5. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).

4.6. Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

4.7. Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

4.8. Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, in dessen Auftrag zu vernichten. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.

4.9. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

5. ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt.

6. SUB- AUFTRAGSVERARBEITER

Der Auftragnehmer kann Sub-Auftragsverarbeiter für IT-Dienstleistungen sowie Softwareerstellung, Beratung udg. hinzuziehen. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub- Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

7. DIVERSES

Änderungen oder Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Sollte eine Vertragsbestimmung unwirksam oder nichtig sein oder werden, dann wird dadurch die Gültigkeit der übrigen Bestimmungen nicht berührt. Die Vertragspartner verpflichten sich vielmehr, die unwirksame oder nichtige Bestimmung durch eine ihr im wirtschaftlichen Zweck möglichst gleichkommende wirksame Regelung zu ersetzen. Für sämtliche Streitigkeiten im Zusammenhang mit oder aus dieser Vereinbarung ist österreichisches Recht anzuwenden.

FIRMA / MAX MUSTERMANN

Funktion / TT.MM.JJJJ

AUFTRAGGEBER	AUFTRAGNEHMER – ESA GMBH
[NAME IN GROßBUCHSTABEN/ FUNKTION/DATUM/UNTERSCHRIFT]	[NAME IN GROßBUCHSTABEN/ FUNKTION/DATUM/UNTERSCHRIFT]

ANLAGE 1

TECHNISCH-ORGANISATORISCHE MAßNAHMEN

VERTRAULICHKEIT

Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B.: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen;
Zugangskontrolle: Schutz vor unbefugter Systembenutzung, z.B.: Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Standard-Berechtigungsprofile auf „need to know-Basis“, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insb. von administrativen Benutzerkonten;
Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.
Klassifikationsschema für Daten: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

INTEGRITÄT

Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement

VERFÜGBARKEIT UND BELASTBARKEIT

Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern;

Rasche Wiederherstellbarkeit;

Löschungsfristen: Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.

VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen; Incident-Response-Management; Datenschutzfreundliche Voreinstellungen;
Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS), Vorabüberzeugungspflicht, Nachkontrollen.