VEREINBARUNG ÜBER EINE AUFTRAGSVERARBEITUNG NACH ART 28 DSGVO

abgeschlossen zwischen

Ortner Reinraumtechnik GmbH
FN 147177 m
Uferweg 7
9500 Villach

im Folgenden „**Auftragnehmer**“ genannt

und

im Folgenden „**Auftraggeber**“ genannt

wie folgt:

1. Gegenstand der Vereinbarung

1.1. Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben:

Verarbeitungen zur Erfüllung eines Vertrags (Art. 6 Abs. 1 Buchst. b DSGVO) und zur

Auftragsabwicklung & Führen eines Kontaktverzeichnises
Verarbeitung und Übermittlung von Daten im Rahmen von Geschäftsbeziehungen mit Auftraggebern, Behörden und Lieferanten, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (z.B. Korrespondenzen oder Verträge) in diesen Angelegenheiten. Verwendung von eigenen Kunden- und Interessentendaten für die Geschäftsanbahnung betreffend das eigene Lieferungs- oder Leistungsangebot, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z. B. Korrespondenz) in dieser Angelegenheit. Bestellungen, Auftragsabwicklung.

Die von Ihnen bereit gestellten Daten sind zur Vertragserfüllung erforderlich. Ohne diese Daten können wir den Vertrag mit Ihnen nicht abschließen.

Verarbeitung zur Erfüllung rechtlicher Verpflichtungen (Art. 6 Abs. 1 Buchst. c DSGVO)

Buchhaltung & Rechnungswesen
Der Zweck der Buchhaltung ist, alle ein- und ausgehenden Zahlungen des Unternehmens sowie sämtliche Dienstleistungs- und Warenflüsse zu belegen.

Daher müssen wir Daten, die wir von Ihnen erhalten haben, aufgrund einer gesetzlichen Verpflichtung verarbeiten, und zwar UGB, BAO, AGBG, UStG.

1.2. Folgende Datenkategorien werden verarbeitet:
Alle Daten, die im Rahmen der oben genannten Tätigkeiten und Zwecke erforderlich sind.

1.3. Folgende Kategorien betroffener Personen:
Kunden, Mitarbeiter, Lieferanten und sonstige Betroffene

2. Dauer der Vereinbarung

Verarbeitungen gemäß diesem Vertrag erfolgen auf unbestimmte Zeit. Die Vereinbarung kann von beiden Parteien gemäß der zugestimmten AGBs gekündigt werden.

2.1. 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.

2.2. 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.

2.3. Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat

2.4. 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 Datenverarbeitung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

2.5. 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).

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

2.7. Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch von ihm 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.

2.8. Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben / 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.

2.9. 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.

3. Ort der Durchführung der Datenverarbeitung

Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw des EWR durchgeführt.

Das angemessene Datenschutzniveau ergibt sich aus

- einem Angemessenheitsbeschluss der Europäischen Kommission nach Art 45 DSGVO.
- einer Ausnahme für den bestimmten Fall nach Art 49 Abs 1 DSGVO.
- verbindlichen internen Datenschutzvorschriften nach Art 47 iVm Art 46 Abs 2 lit b DSGVO.
- Standarddatenschutzklauseln nach Art 46 Abs 2 lit c und d DSGVO.
- genehmigten Verhaltensregeln nach Art 46 Abs 2 lit e iVm Art 40 DSGVO.
- einen genehmigten Zertifizierungsmechanismus nach Art 46 Abs 2 lit f iVm Art 42 DSGVO.
- von der Datenschutzbehörde bewilligte Vertragsklauseln nach Art 46 Abs 3 lit a DSGVO.
- einer Ausnahme für den Einzelfall nach Art 49 Abs 1 Unterabsatz 2 DSGVO.

4. Sub-Auftragsverarbeiter

Der Auftragnehmer kann Sub-Auftragverarbeiter zur Erfüllung des jeweiligen Auftrags hinzuziehen. Er hat den Auftraggeber von der beabsichtigten Heranziehung eines Sub-Auftragsverarbeiters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann. 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. Änderungen des Sub-Auftragverarbeiters sind dem Auftraggeber so rechtzeitig schriftlich bekannt zu geben, dass er dies allenfalls untersagen kann.

5. Sicherheitsmaßnahmen (TOMEN)

5.1. Der Auftragnehmer setzt geeignete technisch-organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus um.

5.2. Der Auftragsverarbeiter prüft in regelmäßigen Abständen, mindestens aber alle 24 Monate, ob durch geeignete technische und organisatorische Maßnahmen in seinem Bereich angemessenes Datenschutzniveau gewährleistet ist.

6. Vertraulichkeit

6.1. **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B.: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen

6.2. **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung, z.B.: Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern

6.3. **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

6.4. **Pseudonymisierung**: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung entfernt, und gesondert aufbewahrt.

7. Integrität

7.1. **Weitergabekontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur

7.2. **Eingabekontrolle**: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement

8. Verfügbarkeit und Belastbarkeit

8.1. **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.

8.2. Rasche **Wiederherstellbarkeit**

9. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

9.1. Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen

9.2. Incident-Response-Management

9.3. Datenschutzfreundliche Voreinstellungen

9.4. **Auftragskontrolle:** Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, Vorabüberzeugungspflicht, Nachkontrollen im Anlassfall.

Für den Auftraggeber: *Für den Auftragnehmer:*

....

Villach, am