Vereinbarung über eine Auftragsverarbeitung gemäß Art. 28 Abs. 3 DSGVO

Der Verantwortliche:	**Der Auftragsverarbeiter:**
	RZA GmbH Hans-Czettel-Straße 1 3950 Gmünd
(im Folgenden „***Verantwortlicher***"), und gemeinsam „die Vertragsparteien"	(im Folgenden „***Auftragsverarbeiter***"

1 Gegenstand der Vereinbarung

1.1 Gegenstand

Die vom Auftragsverarbeiter für den Verantwortlichen übernommenen Datenverarbeitungen beruhen auf dem zwischen den Vertragsparteien abgeschlossenen Vertragsverhältnis (Hauptvertrag). Dieser legt insbesondere Gegenstand, Umfang, Art, Kategorien, der verarbeiteten Daten, die Dauer und den Zweck der Verarbeitung fest. Die nachfolgenden Regelungen des nunmehr ergänzend abgeschlossenen Auftragsverarbeitervertrag finden Anwendung, soweit es sich bei der jeweiligen im Hauptvertrag vereinbarten Leistung um eine Auftragsverarbeitung im Sinne des Artikels 28 DSGVO handelt.

Grundsätzlich obliegen die Rechte und Pflichten aus der Datenschutz-Grundverordnung („***DSGVO***") dem Verantwortlichen. Der Auftragsverarbeiter verpflichtet sich, die Vorgaben der DSGVO und des österreichischen Datenschutzgesetzes und seine ergänzenden Bestimmungen in der jeweils geltenden Fassung zu beachten.

1.2 Art und Zweck der Verarbeitung von Daten

Der Auftragsverarbeiter wird die personenbezogenen Daten ausschließlich auf Basis dieses Vertrags oder wie vom Verantwortlichen gesondert in dokumentierter Weise angewiesen verarbeiten, außer das Unionsrecht oder das Recht eines Mitgliedstaats der Europäischen Union, dem der Auftragsverarbeiter unterliegt, verpflichten den Auftragsverarbeiter zu einer abweichenden Verarbeitung.

2 Dauer der Vereinbarung

Dieser Vertrag ist in seiner Dauer von dem ihm zugrundeliegenden Vertragsverhältnisses abhängig. Einer separaten Kündigung bedarf es nicht.

3 Pflichten des Auftragsverarbeiters

3.1

Der Auftragsverarbeiter verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der Anweisung des Verantwortlichen zu verarbeiten. Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

3.2

Erhält der Auftragsverarbeiter einen behördlichen Auftrag, Daten des Verantwortlichen herauszugeben, so hat er - sofern gesetzlich zulässig - den Verantwortlichen unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragsverarbeiters eines schriftlichen Auftrages.

3.3

Der Auftragsverarbeiter 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 Auftragsverarbeiter aufrecht.

3.4

Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32ff DSGVO ergriffen hat. Konkret handelt es sich hierbei um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Einzelheiten hierzu finden sich unter ANNEX I - Technisch-organisatorische Maßnahmen.

3.5

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten. Dazu gehören 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.

3.6

Der Auftragsverarbeiter ist nach Beendigung der Dienstleistung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten des Verantwortlichen enthalten, dem Verantwortlicher zu übergeben bzw. in dessen Auftrag weiter für ihn aufzubewahren oder zu vernichten. Wenn der Auftragsverarbeiter 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 Verantwortlichen in dem Format, in dem er die Daten vom Verantwortlicher erhalten hat oder in einem anderen, gängigen Format herauszugeben.

3.7

Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Verantwortlichen verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

3.8

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

4 Pflichten des Verantwortlichen

4.1

Für die Erfüllung der Verpflichtungen aus den Betroffenenrechten gemäß den Bestimmungen der gemäß Art. 15 DSGVO (Auskunftsrecht), Art. 16 DSGVO (Recht auf Richtigstellung), Art. 17 DSGVO (Recht auf Löschung), Art. 18 DSGVO (Recht auf Einschränkung), Art. 20 DSGVO (Recht auf Datenübertragbarkeit) und Art. 21 DSGVO (Widerspruchsrecht) gegenüber den Betroffenen ist ausschließlich der Verantwortliche zuständig. Unmittelbare Ansprechperson für den Betroffenen ist daher der Verantwortliche. Der Auftragsnehmer hat aber die notwendigen technischen und organisatorischen Voraussetzungen zu schaffen, damit der Verantwortliche die genannten Verpflichtungen erfüllen kann. Sofern erforderlich, überlässt der Auftragsnehmer dem Verantwortlichen alle dafür notwendigen Informationen.

4.2

Weiters wird festgehalten, dass ausschließlich der Verantwortliche für die Erfüllung allfälliger Genehmigungspflichten hinsichtlich der Verwendung der personenbezogenen Daten im Rahmen dieser Vereinbarung verantwortlich ist. Weiters erklärt der Verantwortliche, dass die gemäß dieser Vereinbarung überlassenen Daten nach den Grundsätzen der Art. 5ff. DSGVO verarbeitet werden insbesondere, dass die Daten rechtmäßig ermittelt wurden und die Verarbeitung der Daten zu den vertragsgegenständlichen Zwecken zulässig ist. Den Auftragsverarbeiter treffen

keinerlei Verpflichtungen gegenüber dem Verantwortlichen oder Dritten, etwa die Rechtmäßigkeit der Verarbeitung personenbezogener Daten zu überprüfen.

4.3

Der Verantwortliche verpflichtet sich, den Auftragsverarbeiter unmittelbar von Änderungen der DSGVO oder der österreichischen Datenschutzgesetze und ergänzender Bestimmungen zu unterrichten. Der Verantwortliche räumt dem Auftragsverarbeiter eine angemessene Frist ein, sich auf geänderte Datenschutzbestimmungen einzustellen.

4.4

Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragsverarbeiter ermittelt. In diesem Fall sowie wenn der Verantwortliche einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.

4.5

Verantwortlicher und Auftragsverarbeiter sind bezüglich der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

4.6

Der Verantwortliche hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.

4.7

Über die Herausgabe oder Löschung der Daten nach Vertragsende muss der Verantwortliche innerhalb einer vom Auftragsnehmer gesetzten Frist entscheiden.

4.8

Mündliche Weisungen bestätigt der Verantwortliche unverzüglich in Schriftform. Der Auftragsverarbeiter hat das Recht mündliche Weisungen solange zu verweigern, als diese schriftlich bestätigt wurden.

5 Support

5.1 Beratung über Fernwartung

Der Verantwortliche ermächtigt den Auftragsverarbeiter die Beratungstätigkeit per Online-Support durchzuführen. Die Verbindung für eine Support-Sitzung wird vom Verantwortlichen aufgebaut und freigeschalten, nachdem dieser den Aufbau und die Freischaltung telefonisch/schriftlich avisiert hat. Die Support-Sitzung erfolgt unter Aufsicht des Verantwortlichen. Der Verantwortliche hat dafür Sorge zu tragen, dass es dabei nicht zu einer Offenlegung personenbezogener Daten kommt. Soweit es aber im Rahmen der konkreten Serviceleistung unvermeidbar ist, kann es zur Einsicht von personenbezogenen Daten kommen. Im Zuge der Sitzung werden die Daten weder kopiert, noch reproduziert oder in irgendeiner anderen Form verarbeitet.

Der Auftragsverarbeiter ist diesbezüglich verpflichtet, Technologien einzusetzen, die nicht nur ein Verfolgen der Tätigkeit auf dem Bildschirm ermöglichen, sondern dem Verantwortlichen auch eine Möglichkeit gibt, die Fernwartungsarbeiten jederzeit zu unterbinden.

Wenn der Verantwortliche bei Fernwartungsarbeiten nicht wünscht, die Tätigkeiten an einem Monitor o.ä. Gerät zu beobachten, wird der Auftragsverarbeiter die von ihm durchgeführten Arbeiten in geeigneter Weise dokumentieren.

Durch Beauftragung des Auftragsverarbeiters durch den Verantwortlichen, kann der Auftragsverarbeiter nicht-personenbezogene Daten, im Bereich der System-Parametrierung, im Zuge der Sitzung verändern. Die Verantwortung trägt zur Gänze der Verantwortliche.

Wird vom Verantwortlichen eine Änderung von personenbezogenen Daten durch den Auftragsverarbeiter gewünscht, erfolgt dies aufgrund der Angaben des Verantwortlichen mit entsprechender Dokumentation durch den Auftragsverarbeiter. Der Auftragsverarbeiter behält sich das Recht vor diesbezüglich eine schriftliche Vereinbarung einzuholen.

5.2 Beratung vor Ort

Bei einer Support-, Beratungs- oder Schulungstätigkeit des Auftragsnehmers vor Ort im Auftrag des Verantwortlichen kann es zur Einsicht von personenbezogenen Daten kommen. Über Beauftragung des Auftragsverarbeiters durch den Verantwortlichen, kann der Auftragsverarbeiter nicht-personenbezogene Daten, im Bereich der System-Parametrierung, im Zuge der vor Ort Beratung verändern. Die Verantwortung trägt zur Gänze der Verantwortliche.

Wird vom Verantwortlichen eine Änderung von personenbezogenen Daten durch den Auftragsverarbeiter gewünscht, erfolgt dies aufgrund der Angaben des Verantwortlichen mit entsprechender Dokumentation durch den Auftragsverarbeiter. Der Auftragsverarbeiter behält sich das Recht vor diesbezüglich eine schriftliche Vereinbarung einzuholen.

5.3 Zur Verfügung stellen von Daten

Sollte es notwendig sein, dass der Verantwortliche dem Auftragsnehmer personenbezogene Daten zur Verarbeitung zur Verfügung stellt, zum Beispiel zur Klärung von Problemfällen, stellt der Auftragsnehmer eine Anleitung zum gesicherten Datenaustausch zur Verfügung. Der Auftragsnehmer wird die im Auftrag des Verantwortlichen verarbeiteten Daten strikt von sonstigen Daten bzw. Datenbeständen trennen. Die Daten werden 21 Tage nach Abschluss des Supportfalls gelöscht. Wenn eine längere Aufbewahrung vom Verantwortlichen gewünscht wird, so muss diese schriftlich dem Auftragsverarbeiter bekannt gegeben werden.

6 Kontrollrechte des Verantwortlichen

6.1

Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DSGVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Aufforderung die erforderlichen Auskünfte zu erteilen und insb. die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

6.2

Sofern diese Angaben zur Erfüllung der gesetzlichen Prüfpflicht nicht ausreichen, hat der Verantwortliche das Recht, im Benehmen mit dem Auftragsverarbeiter Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Diese dürfen nicht im Wettbewerbsverhältnis zum Auftragsverarbeiter stehen. Er hat das Recht, sich durch Stichprobenkontrollen, die 1 Monat im Vorhinein anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen.

6.3

Die Überprüfung findet während der regulären Geschäftszeiten, gemäß den Betriebsrichtlinien der jeweiligen Betriebsstätte des Auftragsverarbeiters statt und darf den Betrieb des Auftragsverarbeiters nicht unangemessen beeinträchtigen. Der Auftragsverarbeiter strengt sich angemessen an, um dem Prüfer die angeforderten Informationen zur Verfügung zu stellen.

6.4

Für die Ermöglichung von Kontrollen durch den Verantwortlichen kann der Auftragsverarbeiter einen Vergütungsanspruch geltend machen. Dieser hat angemessen zu sein.

7 Technisch-organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen („***TOMs***“) unterliegen dem technischen Fortschritt und der Weiterentwicklung. Es ist dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen, soweit das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

Einzelheiten sind ANNEX I zu entnehmen.

8 Ort der Durchführung der Datenverarbeitung

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

9 Sub-Auftragsverarbeiter

Der Verantwortliche erklärt sich einverstanden, dass der Auftragsverarbeiter zur Erfüllung bestimmter Services auch dritte Unternehmen („***Sub-Auftragsverarbeiter***“) zur unmittelbaren Erbringung der Hauptdienstleistung heranziehen kann. Dies bedeutet nicht zwingend, dass im Zuge der Servicierung ein Sub-Auftragsverarbeiter herangezogen wird. Die konkreten Sub-Auftragsverarbeiter sind produktspezifisch im jeweiligen Vertragsverhältnis definiert. Die Sub-Auftragsnehmer können im Detail über die E-Mailadresse dsgvo@rza.at erfragt werden. Der Auftragsverarbeiter muss mit dem Sub-Auftragsverarbeiter gem. Art. 28 Abs. 4 DSGVO einen Vertrag im Sinne des Art. 28 Abs. 3 DSGVO abschließen. In diesem Vertrag hat der Auftragsverarbeiter sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, wie sie dem Auftragsverarbeiter aufgrund dieser Vereinbarung obliegen. Die Auslagerung auf Sub-Auftragsnehmer oder der Wechsel des bestehenden Sub-Auftragsverarbeiters sind zulässig, soweit der Auftragsverarbeiter dies dem Verantwortlichen eine angemessene Zeit vorab schriftlich auf der Webseite www.rza.at/subauftragsverarbeiter anzeigt und der Verantwortliche nicht gegenüber dem Auftragsverarbeiter schriftlich Einspruch gegen die geplante Auslagerung erhebt und die erforderlichen Vereinbarungen zwischen dem Auftragsverarbeiter und dem Sub-Auftragsverarbeiter gemäß des Art. 28 Abs. 4 DSGVO abgeschlossen werden.

10 Schlussbestimmungen

Änderungen und Ergänzungen dieses Vertrags einschließlich dieses Punktes bedürfen der Schriftform sowie der Unterschrift beider Vertragsparteien. Auf alle Rechtsfragen aus oder im Zusammenhang mit diesem Vertrag einschließlich der Frage seines gültigen Zustandekommens und seiner Vor- und Nachwirkungen ist österreichisches Recht unter Ausschluss seiner Verweisungsnormen anzuwenden. Die Vertragsparteien vereinbaren für sämtliche Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung einschließlich der Frage seines gültigen Zustandekommens und seiner Vor- und Nachwirkungen die ausschließliche Zuständigkeit des jeweils sachlich zuständigen Gerichts am Sitz der Gesellschaft. Sollten einzelne Bestimmungen dieses

Vertrags ungültig oder undurchsetzbar sein oder werden, so bleibt der Restvertrag davon unberührt. Diese Bestimmungen gelten als durch gültige und durchsetzbare Regelungen ersetzt, die den von den Vertragsparteien beabsichtigten wirtschaftlichen Zweck am ehesten erreichen.

[Ort], am [Datum]
Für den Verantwortlichen:

.....
[Name samt Funktion]

Amaliendorf, am 24.5.2018
Für den Auftragsverarbeiter:

Reinhard Müllner,
Geschäftsführer
.....

ANNEX I. Technisch-organisatorische Maßnahmen („*TOMs*“)

Vertraulichkeit

Der unbefugte Zutritt zu Datenverarbeitungsanlagen wird mittels Schlüssel und Alarmanlage gewährleistet. Der Zutritt zum Serverraum ist gesondert abgesichert und nur einem sehr eingeschränkten Mitarbeiterkreis möglich. Der Schutz von unbefugten Systembenutzungen wird durch Kennwörter, Firewalls und automatische Sperrmechanismen durchgeführt. Auf Firmennotebooks ist die interne Festplatte verschlüsselt. Der Zugriff auf Dritt-Systeme durch Monitoringapplikationen ist mittels Zwei-Faktor Authentifizierung abgesichert.

Interne Berechtigungen werden nach dem „*need to know*“ Prinzip vergeben. Die Berechtigungen werden periodisch geprüft. Daten die zu unterschiedlichen Zwecken erhoben wurden, werden getrennt verarbeitet. Für externe Kundengeräte sind in der RZA GmbH getrennte und abgesicherte Netzwerksegmente vorhanden.

Integrität

Ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei der elektronischen Datenübertragung wird zwischen Verantwortlichem und Auftragsverarbeiter mittels Verschlüsselung sichergestellt.

Verfügbarkeit und Belastbarkeit

Die Verfügbarkeit wird durch ein mehrstufiges Backupkonzept sichergestellt. Mittels Monitoringsystemen wird die interne Infrastruktur hinsichtlich Security-Vorfälle und div. Systemausfällen überwacht. Durch eine USV-Anlage wird sichergestellt, dass bei Stromausfällen ein geordnetes Herunterfahren der Server ermöglicht. Für den Ein/Austritt sowie Abteilungswechsel von Mitarbeitern existieren Standardprozesse, welche durch die zuständigen Abteilungen eingehalten werden.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Die Mitarbeiter der RZA GmbH werden regelmäßig in Hinblick auf Security Awareness geschult. Es wird keine Auftragsdatenverarbeitung im Sinne von Art 28-DSGVO ohne entsprechende Weisung des Verantwortlichen durchgeführt. Die Systeme werden regelmäßig evaluiert um den Schutz der Rechte, im Verhältnis zum bestehenden Risiko, der betroffenen Personen zu gewährleisten.