R R
Z _

safe data,
great business.

Vereinbarung

betreffend der Beauftragung mit der Datenverarbeitung gemäß Artikel 28 DSGVO zwischen

---

Firmenname

(in weiterer Folge „Verantwortlicher")

und

Raiffeisen Rechenzentrum GmbH

im Firmenverbund der Raiffeisen-Landesbank Steiermark AG

(in weiterer Folge „Auftragsverarbeiter")

Dokument Eigentümer	RRZ GmbH
Version	2.0
Versionsdatum	23.05.2018
Status	FREIGEGEBEN
Vertraulichkeitsklassifizierung	Vertraulich

Dokumentenkontrolle

Dokumentenkontrolle	
Titel	Vereinbarung Datenverarbeitung
Version	2.0
Status (Entwurf / Freigegeben)	FREIGEGEBEN
Ersetzt Version	-
Eigentümer	RRZ GmbH
Revisionsdatum	23.05.2018
Datum der nächsten Revision	-
Dateiname	Vorlage-ADV-DSGVO.docx
Anzahl Seiten	10
Druckdatum	23.05.2018 10:20:00

Dokumentenhistorie

Revisions-datum	Version	Änderungen	Autor	Editor	Begutachter	Genehmiger
12.03.2018	0.1	Erstellung	Hefler	Hefler	Paier	Schlar
23.05.2018	2.0	Anpassung Kate-gorien, Form	Stieg	Stieg	Paier	Paier

1. Diese Vereinbarung wird in Ergänzung zum Rahmen Service Level Agreement zwischen dem Verantwortlichen und dem Auftragsverarbeiter zur Regelung der datenschutzrechtlichen Aspekte geschlossen. Diese Vereinbarung wird für die Laufzeit Rahmen-SLAs geschlossen und endet somit gleichzeitig mit dieser.

2. Der Verantwortliche beauftragt den Auftragsverarbeiter entsprechend der Leistungsvereinbarung mit folgenden Datenverarbeitungen:

   Art und Umfang der Datenverarbeitung sind in den mit dem Kunden geschlossenen letztgültigen Verträgen und Beilagen (Angebot, Rahmen-SLA, Leistungsbeschreibung und AGB) definiert.

- Bei der Auftragsdatenverarbeitung kommt es zur Verarbeitung folgender Arten personenbezogener Daten der folgenden Kategorien betroffener Personen:

  .1. Die jeweils zutreffenden Personenkategorien werden in nachfolgender Tabelle mit einem X gekennzeichnet.

X	Zutreffende Kategorie der betroffenen Personen	Datenarten (personenbezogene Daten)
	Beispiele: *Auftraggeber/Verantwortlicher, Kunden des Auftraggebers/des Verantwortlichen, Geschäftspartner, Lieferanten, Mitarbeiter, etc.*	***Beispiele:*** *Kontaktdaten, Abrechnungsdaten, Protokolldaten, Vertragsdaten, Zahlungsdaten, Bild- und Tonaufzeichnungen, etc.*

X	Zutreffende Kategorie der betroffenen Personen	Datenarten (personenbezogene Daten)

.2. Bestehen vertraglich fixierte temporäre oder dauerhafte Zutrittsberechtigungen zum Rechenzentrum, werden seitens der RRZ GmbH Kopien von Ausweisdokumenten wie bspw. Reisepässen zum Zweck der Identitätsfeststellung sowie Biometrische Daten zum Zweck der Zutrittssteuerung gespeichert und verarbeitet.

X	Zutreffende Kategorie der betroffenen Personen	Datenarten (personenbezogene Daten)
	Auftraggeber/Verantwortlicher	• Kontaktdaten • Daten zu Identitäts- und Reisedokumenten • Biometrische Daten • Persönliche Detailangaben • Daten zu Marketing und Vertrieb • Elektron. Protokoll- u. Identifikationsdaten • Elektronische Standort- und Bewegungsdaten • Bild- und/oder Tonaufzeichnungen
	Lieferanten des Auftraggebers/des Verantwortlichen	• Kontaktdaten • Daten zu Identitäts- und Reisedokumenten • Biometrische Daten • Persönliche Detailangaben • Daten zu Marketing und Vertrieb • Elektron. Protokoll- u. Identifikationsdaten • Elektronische Standort- und Bewegungsdaten • Bild- und/oder Tonaufzeichnungen

3. Der Auftragsverarbeiter verpflichtet sich, die Regelungen des jeweils geltenden österreichischen und europäischen Datenschutzrechts einzuhalten. Hierzu gehören insbesondere folgende Verpflichtungen:

   - Der Auftragsverarbeiter verpflichtet sich, personenbezogene Daten nur entsprechend dieser Vereinbarung oder sonst auf dokumentierte Weisung des Verantwortlichen zu verarbeiten, sofern er nicht durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

   - Die Datenverarbeitung findet ausschließlich innerhalb der EU statt. Die Datenverarbeitung in einem Drittland außerhalb der EU bedarf der vorherigen schriftlichen Zustimmung des Verantwortlichen auf Seiten des Kunden und der Einhaltung der Voraussetzungen der Artikel 44 ff. DSGVO.

   - Der Auftragsverarbeiter leistet Gewähr, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragsverarbeiter aufrecht. Die Verpflichtung zur Verschwiegenheit ist auch für Daten von juristischen Personen und handelsrechtlichen Personengesellschaften einzuhalten.

   - Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er ausreichende technische und organisatorische Maßnahmen im Sinne des Artikels 32 DSGVO ergriffen hat, damit ein dem Risiko angemessener Schutz personenbezogener Daten hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit der Daten sowie der Belastbarkeit der Systeme gewährleistet ist und verhindert wird, dass Daten ordnungswidrig verwendet oder Dritten unbefugt zugänglich werden. Die vom Auftragsverarbeiter einzuhaltenden technischen und organisatorischen Maßnahmen sind in Anlage 1 näher beschrieben. Der Auftragsverarbeiter hat die Umsetzung der technischen und organisatorischen Maßnahmen zu dokumentieren.

     Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternativ adäquate Maßnahmen umzusetzen.

Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

- Der Auftragsverarbeiter kann ein anderes Unternehmen (Unterauftragsverarbeiter) nur dann mit der Durchführung von Verarbeitungen betrauen, wenn der Verantwortliche auf Seiten des Kunden im Vorhinein gesondert schriftlich zustimmt.

- Bei der Nutzung von Cloudservices des Auftragsverarbeiters erteilt der Verantwortliche auf Seiten des Kunden hiermit die allgemeine Zustimmung zur Beauftragung weiterer Auftragsverarbeiter. Der Auftragsverarbeiter verpflichtet sich jedoch dazu, den Verantwortlichen stets über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter zu informieren. Der Verantwortliche hat die Möglichkeit, gegen derartige Änderungen Einspruch zu erheben.

  Erbringt der Unterauftragsverarbeiter die vereinbarte Leistung außerhalb der EU, stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

  Nimmt der Auftragsverarbeiter die Dienste eines Unterauftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten des Verantwortlichen auszuführen, so werden diesem Unterauftragsverarbeiter im Wege eines Vertrags dieselben Datenschutzpflichten auferlegt, die in diesem Vertrag festgelegt sind. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes Unterauftragsverarbeiters.

- Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Person, insbesondere auf Auskunft, Richtigstellung oder Löschung (Art 15 bis 22 DSGVO), nachzukommen.

- Weiters verpflichtet sich der Auftragsverarbeiter, unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten betreffend die Sicherheit personenbezogener Daten zu unterstützen.

- Im Falle einer Datenschutzverletzung hat der Auftragsverarbeiter unverzüglich den Verantwortlichen zu informieren. Der Auftragsverarbeiter hat den Verantwortlichen bei der Meldung der Datenschutzverletzung an

die Aufsichtsbehörde und an die Betroffenen zu unterstützen sowie sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen.

- Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung seiner Pflichten bei einer Datenschutzfolgenabschätzung (Art 35 DSGVO). Der Auftragsverarbeiter stellt dem Verantwortlichen dazu insbesondere relevante Informationen zur Auftragsdatenverarbeitung sowie zu den technischen und organisatorischen Maßnahmen zur Verfügung, unterstützt bei der Bewertung der Risiken und allfälligen Anpassungen der technischen und organisatorischen Maßnahmen.

- Der Auftragsverarbeiter ist nach Abschluss der Erbringung der Verarbeitungsleistungen verpflichtet, alle personenbezogenen Daten, einschließlich aller in seinen Besitz gelangten Unterlagen, von ihm selbst erstellte Verarbeitungsergebnisse sowie Datenbestände, die im Zusammenhang mit der Auftragsdatenverarbeitung stehen, nach Wahl des Verantwortlichen entweder datenschutzgerecht zu löschen bzw. zu vernichten oder dem Verantwortlichen auszuhändigen.

- Die Rückgabe- bzw. Löschungspflicht gemäß dem vorigen Absatz gilt nicht, sofern nicht nach dem Unionsrecht oder dem Recht eines Mitgliedstaates der EU eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

- Der Auftragsverarbeiter wird dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in dieser Vereinbarung niedergelegten Pflichten zur Verfügung stellen und auf Aufforderung alle erforderlichen Auskünfte erteilen. Der Auftragsverarbeiter ermöglicht Überprüfungen und Inspektionen durch den Verantwortlichen oder einen von diesem beauftragten Prüfer. Die entstehenden Aufwände bei Auditierungen werden zu den jeweils gültigen Stundensätzen in Rechnung gestellt. Bei sachlichen in der Person des Dritten begründeten Einwänden des Auftragsverarbeiters kann dieser der Auswahl des Dritten widersprechen.

  Bei ähnlich gelagerten Auftragsverarbeitungen für mehrere Verantwortliche gestattet der Auftragsverarbeiter auch Überprüfungen durch von den Verantwortlichen gemeinsam beauftragte Prüfer oder er beauftragt selbst auf Wunsch oder mit Einverständnis der Verantwortlichen und auf deren Rechnung solche Prüfungen durch geeignete Stellen (z.B. Innenrevisoren, Wirtschaftsprüfer, IT-Sicherheits-Auditoren, Datenschutzauditoren, Qualitätsauditoren) und stellt die Prüfungsberichte den Verantwortlichen und deren Prüfern sowie auf Verlangen auch den für die Verantwortlichen zuständigen Aufsichtsbehörden zur Verfügung.

- Der Auftragsverarbeiter unterstützt den Verantwortlichen bei Untersuchungen oder Verfahren von Aufsichtsbehörden sowie bei der Erfüllung von Pflichten gegenüber Aufsichtsbehörden. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Untersuchungen oder Maßnahmen von Aufsichtsbehörden im Zusammenhang mit der Auftragsverarbeitung für den Verantwortlichen. Soweit der Verantwortliche seinerseits Untersuchungen oder Maßnahmen von Aufsichtsbehörden, Verwaltungs- oder Strafverfahren oder Ansprüchen von betroffenen Personen oder Dritten im Zusammenhang mit der Auftragsverarbeitung ausgesetzt ist, unterstützt ihn der Auftragsverarbeiter nach besten Kräften.
- Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich informieren, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere geltende Datenschutzbestimmungen verstößt. Der Auftragsverarbeiter kann die Durchführung der entsprechenden Weisung aussetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung den Regelungen des Rahmen-SLA und der Leistungsbeschreibung vor.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

[Diese Vereinbarung tritt mit 25. Mai 2018 in Kraft.]

Anlage 1; Technische und organisatorische Maßnahmen

Für den Verantwortlichen: Für den Auftragsverarbeiter:

.....
Ort, Datum

.....	.....	.....
Unterschrift	Unterschrift	Unterschrift
.....	DI ULFRIED PAIER	DI (FH) DIETMAR SCHLAR
Name		

1. Anlage 1: Technisch-organisatorische Maßnahmen

1.1. Vertraulichkeit (Art 32 Abs 1 lit b DSGVO)

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

- **Zugangskontrolle**
  Schutz vor unbefugter Systembenutzung, z.B. (sichere) 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;

- **Trennungskontrolle**
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;

- **Pseudonymisierung** (Art 32 Abs 1 lit a DSGVO; Art 25 Abs 1 DSGVO)
  Sofern für die jeweilige Datenverarbeitung erforderlich oder zweckmäßig, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, sodass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer konkreten betroffenen Person zugeordnet werden können, und diese zusätzlichen Informationen werden gesondert aufbewahrt und unterliegen entsprechenden technischen und organisatorischen Maßnahmen;

- **Klassifikationsschema für Daten**
  Beachtung der vom Verantwortlichen vorgegebenen Klassifikationsschemata (z.B.: geheim/vertraulich/intern/öffentlich);

- **Technische Löschkonzept-Einstellungen**
  Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.;

1.2. Integrität (Art 32 Abs 1 lit b DSGVO)

- **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;

1.3. Verfügbarkeit und Belastbarkeit (Art 32 Abs 1 lit b DSGVO)

- **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** (Art 32 Abs 1 lit c DSGVO);

1.4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art 32 Abs 1 lit d DSGVO; Art 25 Abs 1 DSGVO)

- **Datenschutz-Management**
  einschließlich regelmäßiger Mitarbeiter-Schulung;

- **Incident-Response-Prozesse**

- **Datenschutzfreundliche Voreinstellungen** (Art 25 Abs 2 DSGVO)

- **Auftragskontrolle**
  Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Verantwortlichen, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.