# RZL DSGVO Auftragsverarbeiter-Rahmenvereinbarung

Zwischen dem RZL Anwender

.....

.....

.....

.....

(im Folgenden „Verantwortlicher“)

und der

**RZL Software GmbH**
**Hannesgrub Nord 35**
**4911 Tumeltsham**

(im Folgenden „Auftragsverarbeiter“)

Der Auftragsverarbeiter hat sich verpflichtet, die in Anhang 1 gewählten und beschriebenen Datenverarbeitungen gegenüber dem Verantwortlichen zu erbringen. Für die Zwecke dieser Vereinbarung gelten die Begriffsdefinitionen der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679).

1. Weisungsrecht. Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – sofern er nicht durch das Recht der 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.

2. Vertraulichkeit. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

3. Datensicherheit. Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er ausreichende Sicherheitsmaßnahmen ergriffen hat, um zu verhindern, dass Daten ordnungswidrig verwendet oder Dritten unbefugt zugänglich werden. Außerdem erklärt der Auftragsverarbeiter, dass er alle gemäß Artikel 32 Datenschutz-Grundverordnung erforderlichen Maßnahmen ergreift. Diese Maßnahmen schließen im Besonderen die in Anhang 2 beschriebenen Maßnahmen ein.

4. Meldung einer Verletzung des Schutzes personenbezogener Daten. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über eine Verletzung des Schutzes personenbezogener Daten, die der Auftragsverarbeiter im Auftrag des Verantwortlichen verarbeitet. Diese Meldung soll zumindest beschreiben:
   a. die Art der Verletzung des Schutzes personenbezogener Daten, einschließlich der Kategorien und der Zahl der betroffenen Personen und der Zahl der betroffenen Datensätze;
   b. die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

c. die vom Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten sowie gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen Auswirkungen.

Im Falle einer Verletzung des Schutzes personenbezogener Daten unterstützt der Auftragsverarbeiter den Verantwortlichen dabei, Maßnahmen zur Wiederherstellung der Datensicherheit zu treffen sowie die Verletzung zu beenden.

5. Sub-Auftragsverarbeitung. Die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter oder Sub-Auftragsverarbeiter (im Folgenden zusammen „Sub-Auftragsverarbeiter") bedarf der vorhergehenden ausdrücklichen schriftlichen Zustimmung des Verantwortlichen [1]. Nimmt der Auftragsverarbeiter einen anderen Sub-Auftragsverarbeiter in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem Sub-Auftragsverarbeiter im Wege eines schriftlichen Vertrags dieselben Datenschutzpflichten auferlegt, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen des anwendbaren Datenschutzrechts erfolgt. Außerdem überprüft der Auftragsverarbeiter regelmäßig die Einhaltung der Datenschutzpflichten durch den Sub-Auftragsverarbeiter und teilt dem Verantwortlichen jede etwaige Verletzung dieser Pflichten unverzüglich mit. Der Auftragsverarbeiter hat in einem solchen Fall die Sub-Auftragsverarbeitung zu beenden, wenn dies vom Verantwortlichen verlangt wird. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

6. Unterstützung. Der Auftragsverarbeiter unterstützt den Verantwortlichen durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung der Pflichten des Verantwortlichen bei Anträgen auf Wahrnehmung der Betroffenenrechte gemäß Kapitel III der Datenschutz-Grundverordnung. Der Auftragsverarbeiter stellt seine Unterstützung innerhalb von fünf Arbeitstagen ab Anfrage des Verantwortlichen beim Auftragsverarbeiter bezüglich eines Antrages einer betroffenen Person auf Wahrnehmung ihrer Betroffenenrechte zur Verfügung. Darüber hinaus unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung seiner Pflichten gemäß dem anwendbaren Datenschutzrecht, einschließlich Artikel 32 bis 36 Datenschutz-Grundverordnung.

7. Rückgabe von personenbezogenen Daten. Nach Wahl des Verantwortlichen löscht der Auftragsverarbeiter nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten oder gibt diese in elektronischem, strukturierten, üblicherweise gebrauchten und wiederverwendbaren Format zurück, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

8. Überprüfung. Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten unentgeltlich zur Verfügung.

09.05.2018

| | |
|---|---|
| Verantwortlicher – RZL Anwender | Auftragsverarbeiter RZL Software GmbH<br>Hannesgrub Nord 35, 4911 Tumeltsham |

[1] Alternative für Fälle, in denen Sub-Auftragsverarbeiter üblicherweise vorkommen (z.B. Cloud-Anbieter) oder es in konkreten Werkverträgen so vorgesehen ist: „Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter oder Sub-Auftragsverarbeiter (im Folgenden zusammen „Sub-Auftragsverarbeiter") einen Monat vor der beabsichtigten Änderung, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen in diesem Zeitraum Einspruch zu erheben."

# Anhang 1 zur RZL DSGVO Auftragsverarbeiter-Rahmenvereinbarung

**Betroffene Personen**

Die übermittelten personenbezogenen Daten betreffen je nach RZL Programm eine oder mehrere der folgenden Kategorien betroffener Personen:

Derzeitige, ehemalige und zukünftige Arbeitnehmer, arbeitnehmerähnliche Personengruppen, freie Dienstnehmer, Volontäre und Praktikanten; Bewerber / derzeitige, ehemalige und zukünftige Klienten/Kunden/Mandanten und deren Angehörige und Mitarbeiter / derzeitige, ehemalige und zukünftige Lieferanten und deren Mitarbeiter / derzeitige, ehemalige und zukünftige Kontaktpersonen von Behörden, Ämtern, Banken, Rechtsanwälten sowie im Programm verwaltete Kontakten.

**Kategorien von Daten**

Die übermittelten personenbezogenen Daten gehören je nach RZL Programm zu einer oder mehreren der folgenden Datenkategorien:

Stammdaten- und Personendaten sowie Fotos eigener Mitarbeiter, Klienten/Mandanten/Kunden und deren Mitarbeitern, Lieferanten, Kontaktdaten von Mitarbeitern bei Behörden, Ämtern, Banken. Unternehmensspezifische Daten des Klienten/Mandanten/Kunden, Daten iZm der Durchführung der Lohnabrechnung, Buchhaltung, Anlagenabschreibung, Jahresabschluss bzw. Bilanzierung, der Erstellung von Steuererklärungen, Kostenrechnung, Zahlungsverkehr, Kontaktpersonen bei den Klienten/Mandanten/Kunden, Daten iZm mit steuerlicher Spezialberatung, Daten iZm finanzstrafrechtlicher Beratung und jene iZm der Unterstützung bei Finanzstrafverfahren, Daten iZm einer allfälligen Unternehmensstruktur von Klienten/Mandanten/Kunden und deren Gesellschaftern, Daten iZm der Prüfung diverser Verträge, Finanzierungs- und Zahlungsbedingungen, Mahn- und Klagsdaten, Daten iZm der Durchführung des Mahnwesens im Auftrag des Mandanten.

**Daten der besonderen Kategorie**

Die übermittelten personenbezogenen Daten umfassen je nach RZL Programm eine oder mehrere der folgenden Daten besonderer Kategorie: Gesundheitsdaten (Sozialversicherungsnummer, Krankenstände, etc…), Gewerkschaftszugehörigkeit

*Der Verantwortliche definiert hier durch Ankreuzen*
*alle vom Auftragsverarbeiter bezogenen Dienstleistungen für die Punkte:*
Gegenstand der Verarbeitung *und* Verarbeitungszwecke.

☒ **Für den RZL Support, inkl. Schulung und Datenkonvertierung:**

**Gegenstand der Verarbeitung und Verarbeitungsmaßnahmen für den RZL Support:**

Die übermittelten personenbezogenen Daten werden wahlweise einer oder mehreren der folgenden grundlegenden Verarbeitungsmaßnahmen unterzogen:
Sicherstellung eines reibungslosen Ablaufs der RZL Programme sowie Hilfestellung auf Anfragen des Verantwortlichen. Es erfolgt wahlweise – im Rahmen dieser Hilfestellung – telefonische Beratung, eine Remote-Verbindung (Fernwartung), eine Übermittlung des Datensatzes oder Einsichtnahme vor Ort (z.B. im Rahmen einer Schulung) ausschließlich auf Veranlassung des Verantwortlichen.

**Verarbeitungszwecke für den RZL Support:**

Es werden keine personenbezogenen Daten direkt durch RZL verarbeitet. Es besteht im Rahmen der Hilfestellung bzw. Schulung vor Ort oder online) lediglich die Möglichkeit, personenbezogenen Daten ungewollt einzusehen.

☐ **Für die RZL Cloud Services:**

### Gegenstand der Verarbeitung und Verarbeitungsmaßnahmen für RZL Cloud Services

Die verarbeiteten personenbezogenen Daten werden wahlweise einer oder mehreren der folgenden grundlegenden Verarbeitungsmaßnahmen unterzogen:
Ferntechnischer Zugang zu RZL Programmen, mit denen der Verantwortliche eigenverantwortlich die Verarbeitung sowie Speicherung seiner Daten im Rahmen der Funktionalitäten der RZL Programme (Finanzbuchhaltung, Personalverrechnung bzw. Lohn-/Gehaltsverrechnung, etc…) vornehmen kann. Zugriff auf Daten seitens des Auftragsverarbeiters erfolgt ausschließlich auf Weisung des Verantwortlichen.

### Verarbeitungszwecke für RZL Cloud Services

Die verarbeiteten personenbezogenen Daten werden zu folgenden Zwecken des Verantwortlichen verarbeitet: Es erfolgt (für die RZL Cloud Services) nur die Bereitstellung, Pflege und Wartung der RZL Programme sowie des notwendigen Speicherplatzes für die Daten des Verantwortlichen.

☐ **Für das RZL Klientenportal:**

### Gegenstand der Verarbeitung und Verarbeitungsmaßnahmen für das RZL Klientenportal

Die verarbeiteten personenbezogenen Daten werden wahlweise einer oder mehreren der folgenden grundlegenden Verarbeitungsmaßnahmen unterzogen:

Verschlüsselter Internet Browser Zugang zum RZL Klientenportal, mit denen der Verantwortliche eigenverantwortlich die Verarbeitung sowie Speicherung seiner Daten im Rahmen der Funktionalitäten des RZL Klientenportals (Dokumentenaustausch, Kontierungen, ELDA-Mindestangabenmeldungen, …) des RZL Klientenportal vornehmen kann.

### Verarbeitungszwecke für das RZL Klientenportal

Die verarbeiteten personenbezogenen Daten werden zu folgenden Zwecken des Verantwortlichen verarbeitet: Es erfolgt nur die Bereitstellung, Pflege und Wartung des RZL Klientenportal sowie des notwendigen Speicherplatzes für die Daten des Verantwortlichen.

# Anhang 2 zur RZL DSGVO Auftragsverarbeiter-Rahmenvereinbarung

# Sicherheitsmaßnahmen

## Präventive Sicherheitsmaßnahmen – Maßnahmen zur Verhinderung eines erfolgreichen Angriffs

### Technische Maßnahmen

- **Logische Zugriffskontrolle**: Die Vergabe von Zugriffsberechtigungen erfolgt nach dem „Need-to-Know"-Prinzip.
- **Authentifizierung**: Jeglicher Zugriff auf personenbezogene Daten erfolgt ausschließlich nach einer erfolgreichen Authentifizierung.
- **Passwortsicherheit**: Soweit Passwörter zur Authentifizierung eingesetzt werden, sollten diese mindestens 8 Zeichen lang sein und aus Klein- und Großbuchstaben, Zahlen und Sonderzeichen bestehen. Passwörter werden ausschließlich verschlüsselt gespeichert.
- **Verschlüsselung auf dem Übertragungsweg**: Personenbezogene Daten werden auf dem Übertragungsweg über das Internet verschlüsselt, zumindest soweit es sich um Daten der Lohnverrechnung oder sensible Daten handelt.
- **Verschlüsselung mobiler Geräte**: Mobile Endgeräte und mobile Datenträger werden verschlüsselt, zumindest soweit auf diesen Geräten Daten der Lohnverrechnung oder sensible Daten gespeichert werden.
- **Netzwerksicherheit**: Es wird eine Firewall eingesetzt, welche das interne Netzwerk vom Internet trennt und – soweit möglich – eingehenden Netzwerkverkehr blockiert.
- **Maßnahmen gegen Schadsoftware**: Es wird nach Möglichkeit auf allen Systemen Anti-Viren Software eingesetzt. Alle eingehenden E-Mails werden automatisch auf Schadsoftware gescannt.
- **Management von Sicherheitslücken**: Soweit möglich, wird auf allen Geräten die automatische Installation von Sicherheitsupdates aktiviert. Ansonsten erfolgt die Installation kritischer Sicherheitsupdates binnen 3 Arbeitstagen, die Installation von Sicherheitsupdates mittlerer Kritikalität binnen 25 Arbeitstagen und die Installation von Sicherheitsupdates geringer Kritikalität binnen 40 Arbeitstagen.

### Organisatorische Maßnahmen

- **Klare Zuständigkeiten**: Interne Zuständigkeiten für Fragen der Datensicherheit werden definiert.
- **Verschwiegenheitspflicht der Dienstnehmer**: Die Dienstnehmer werden über die Dauer ihres Dienstverhältnisses hinaus zur Verschwiegenheit verpflichtet. Insbesondere werden sie dazu verpflichtet, personenbezogene Daten nur auf ausdrückliche Anweisung des Verantwortlichen an Dritte zu übermitteln.
- **Schulungen und Informationsmaßnahmen**: Die Dienstnehmer werden zu Fragen der Datensicherheit (intern oder extern) geschult und angemessen über Fragen der Datensicherheit informiert (z.B. Passwortsicherheit).

- **Geordnete Beendigung des Dienstverhältnisses**: Bei Beendigung des Dienstverhältnisses erfolgt eine unverzügliche Sperrung aller Accounts des ausscheidenden Dienstnehmers sowie eine Abnahme aller Schlüssel des ausscheidenden Dienstnehmers.
- **Verwaltung von Computer-Hardware**: Es werden Aufzeichnungen darüber geführt, welchem Mitarbeiter welche Endgeräte (z.B. PC, Laptop, Mobiltelefon) zugewiesen wurden.
- **Eingabekontrolle**: Es bestehen Verfahren zur Kontrolle der Richtigkeit der eingegebenen personenbezogenen Daten.
- **Keine Doppelverwendung von Benutzer-Accounts**: Jede Person sollte ihren eigenen Benutzer-Account haben – das Teilen von Benutzer-Accounts ist untersagt.
- **Keine unnötige Verwendung administrativer Accounts**: Benutzer-Accounts mit administrativen Rechten werden nur in Ausnahmefällen verwendet – die reguläre Nutzung von IT-Systemen erfolgt ohne administrative Rechte.
- **Auswahl der Dienstleister**: Bei der Auswahl von Dienstleistern wird das vom Dienstleister gebotene Datensicherheitsniveau berücksichtigt. Der Einsatz eines Dienstleisters, der als Auftragsverarbeiter einzustufen ist, erfolgt nur nach Abschluss einer Auftragsverarbeiter-Vereinbarung.
- **Sichere Datenentsorgung**: Papier, welches personenbezogene Daten enthält, wird grundsätzlich geschreddert bzw. einem externen Dienstleister zur sicheren Vernichtung übergeben. Datenträger werden vor ihrer fachgerechten Entsorgung vollständig überschrieben oder physisch zerstört, sodass die darauf gespeicherten Daten nicht wieder hergestellt werden können.

## Physische Maßnahmen

- **Physische Zugangskontrolle**: Das Betreten der Betriebsräumlichkeiten ist für betriebsfremde Personen nur in Begleitung einer betriebsangehörigen Person zulässig.
- **Einbruchssicherheit**: Die Zugänge zu den Betriebsräumlichkeiten verfügen über einen angemessenen Einbruchsschutz (z.B. eine Sicherheitstüre höherer Widerstandsklasse).
- **Besonderer Schutz von Computer-Hardware**: Der Zugang zu Räumlichkeiten, in denen sich Computer-Server befinden, ist durch besondere Maßnahmen gesichert (z.B. zusätzliches Schloss).
- **Schlüsselverwaltung**: Schlüssel, welchen den Zugang zu den Betriebsräumlichkeiten oder Teilen derselben ermöglichen, werden nur an besonders vertrauenswürdige Personen ausgehändigt und dies auch nur soweit und solange diese Personen tatsächlich einen eigenen Schlüssel benötigen.

## Detektive Sicherheitsmaßnahmen – Maßnahmen zur Erkennung eines Angriffs

### Technische Maßnahmen

- **Scans nach Schadsoftware**: Die IT Systeme werden regelmäßig Überprüfungen nach Schadsoftware (z.B. Anti-Viren-Scans) unterzogen, um Schadsoftware zu identifizieren, welche ein IT-System bereits kompromittiert hat.
- **Automatische Prüfung von Logfiles**: Soweit die Sicherheits-Logfiles mehrerer Systeme auf einem System zentralisiert gesammelt werden, erfolgt eine automatisierte Auswertung der Logfiles, um mögliche Sicherheitsverletzungen zu erkennen.
- **Sicherheits-Mailing-Listen**: Es wird sichergestellt, dass ein Mitarbeiter des Unternehmens oder ein externer Dienstleister einschlägige Mailing-Listen für die Bekanntgabe neuer IT-Sicherheits-Bedrohungen abonniert (z.B. Mailing-Listen der Hersteller der verwendeten Software), um über die aktuelle Bedrohungslage in Kenntnis zu sein.

### Organisatorische Maßnahmen

- **Erkennung von Sicherheitsverletzungen durch Dienstnehmer**: Alle Dienstnehmer werden instruiert, wie und woran sie Sicherheitsverletzung erkennen können (z.B. Meldungen von Anti-Viren-Software, nicht mehr auffindbare Computer-Hardware).
- **Betriebsfremde Personen**: Alle Dienstnehmer werden instruiert, betriebsfremde Personen anzusprechen, sollten sie in den Betriebsräumlichkeiten angetroffen werden.
- **Audits**: Es werden regelmäßige Audits durchgeführt (z.B. Prüfung, ob alle kritischen Sicherheits-Updates installiert wurden). Insbesondere erfolgt eine regelmäßige Prüfung der erteilten Zugriffs- und Zutrittsberechtigungen (welchem Mitarbeiter ist welcher Benutzer-Account mit welchen Zugriffsrechten zugewiesen; welche Personen verfügen über welche Schlüssel).
- **Manuelle Prüfung von Logfiles**: Soweit Logfiles geführt werden (z.B. über erfolglose Authentifizierungsversuche), werden diese in regelmäßigen Abständen geprüft.

### Physische Maßnahmen

- **Brandmelder**: Sofern dies aufgrund der Größe und Beschaffenheit der Betriebs-räumlichkeiten angemessen ist, wird ein Brandmelder installiert, der durch Rauch automatisch ausgelöst wird.

## Reaktive Sicherheitsmaßnahmen – Maßnahmen zur Reaktion auf einen Angriff

### Technische Maßnahmen

- **Datensicherung**: Es werden regelmäßig Datensicherungen erstellt und sicher aufbewahrt.
- **Datenwiederherstellungskonzept**: Es wird ein Konzept zur raschen Wiederherstellung von Datensicherungen entwickelt, um nach einer Sicherheitsverletzung zeitnah den regulären Betrieb wieder herstellen zu können.

- **Automatische Entfernung von Schadsoftware**: Die eingesetzte Anti-Viren-Software verfügt über die Funktion, Schadsoftware automatisch zu entfernen.

### Organisatorische Maßnahmen

- **Meldepflicht für Dienstnehmer**: Alle Dienstnehmer werden angewiesen, Sicherheitsverletzungen unverzüglich an eine zuvor definierte interne Stelle bzw. Person zu melden.
- **Meldepflicht für externe Dienstleister**: Allen Dienstleistern wurden Kontaktdaten für die Meldung von Sicherheitsverletzungen mitgeteilt.
- **Prozess für die Reaktion auf Sicherheitsverletzungen**: Es wird durch einen geeigneten Prozess sichergestellt, dass Sicherheitsverletzungen innerhalb von 72 Stunden ab Kenntnis von der Sicherheitsverletzung an die Datenschutzbehörde gemeldet werden können. Insbesondere sind allen Dienstnehmern die Notfall-Telefonnummern der zu involvierenden Personen bekannt zu geben (z.B. Notfall-Telefonnummer für den IT-Support).

### Physische Maßnahmen

- **Feuerlöscher**: In den Betriebsräumlichkeiten gibt es eine geeignete Anzahl an Feuerlöschern. Allen Dienstnehmern ist bekannt, wo sich die Feuerlöscher befinden.
- **Feueralarm**: Soweit es keinen Brandmelder gibt, der über keine automatische Verbindung zur Feuerwehr verfügt, wird durch einen angemessenen Prozess sichergestellt, dass die Feuerwehr manuell verständigt werden kann.

## Abschreckende Sicherheitsmaßnahmen – Maßnahmen zur Minderung der Angreifermotivation

### Technische Maßnahmen

- **Automatische Warnmeldungen**: Nutzer erhalten automatische Warnmeldungen bei risikoträchtiger IT-Nutzung (z.B. durch den Webbrowser, wenn eine verschlüsselte Website kein korrektes SSL/TLS-Zertifikat verwendet).

### Organisatorische Maßnahmen

- **Sanktionen bei Angriffen durch eigene Dienstnehmer**: Alle Dienstnehmer werden darüber informiert, dass Angriffe auf betriebseigene IT-Systeme nicht toleriert werden und schwerwiegende arbeitsrechtliche Konsequenzen, wie insbesondere eine Entlassung nach sich ziehen können.