Vertrag

zwischen

_____
_____
_____

Kontaktdaten Datenschutz

Ansprechpartner/in: _____
Mail: _____
Tel.: _____
Vertragsnummer des Hauptvertrags: _____

-nachstehend Auftraggeber genannt- und der

RIB IMS GmbH
Erlenstraße 80
46539 Dinslaken

-nachstehend Auftragnehmer genannt-

Kontaktdaten Datenschutz

Ansprechpartnerin: Frau Janna Büscher
Mail: datenschutz@rib-ims.com
Tel.: +49 02064 4896-68

Präambel

Im Rahmen der Softwarepflege und Problemanalyse ist der Zugriff des Auftragnehmers auf personenbezogene Daten des Auftraggebers nicht auszuschließen oder teilweise auch notwendig. Gemäß Artikel 28 EU Datenschutzgrundverordnung (DSGVO) ist ein entsprechender Vertrag zu schließen (siehe Kurzpapier 13 der unabhängigen Datenschutzbehörden des Bundes und der Länder "DSK"). Dazu dient die vorliegende Vereinbarung.

§ 1 Gegenstand der Vereinbarung

(1) Der Auftragnehmer erbringt für den Auftraggeber Supportleistungen im Rahmen eines bestehenden Dienstleistungsvertrages im Bereich der Software- und Datenbankpflege. Diese Leistungen können sowohl beim Auftraggeber vor Ort als auch über den Weg der Fernwartung erbracht werden.
(2) Im Rahmen dieser Dienstleistung kann es nötig werden, auf personenbezogene Daten des Auftraggebers zuzugreifen. Die Art der personenbezogenen Daten und die Kategorie betroffener Personen lauten:

Art der personenbezogenen Daten

☐ Personenstammdaten
☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
☐ Vertragsstammdaten (Vertragsbezeichnung, Produkt- bzw. Vertragsinteresse)
☐ Kundenhistorie
☐ Vertragsabrechnungs- und Zahlungsdaten
☐ Planungs- und Steuerungsdaten
☐ Auskunftsdaten (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
☐ Sonstige: _____
_____
_____
_____

Kategorien betroffener Personen

☐ Kunden
☐ Interessenten
☐ Abonnenten
☐ Beschäftigte
☐ Lieferanten
☐ Handelsvertreter
☐ Ansprechpartner
☐ Sonstige: _____
_____
_____

(3) Die Nutzung dieser Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen nach Kapitel V DSGVO erfüllt sind.

§ 2 Pflichten des Auftraggebers

(4) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Er bleibt der „Verantwortliche" im Sinne der DSGVO. Insofern hat der Auftragnehmer Anfragen Betroffener unverzüglich an den Auftraggeber weiterzuleiten.
(5) Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen.
(6) Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.
(7) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
(8) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers ausschließlich im zur Erbringung der vereinbarten Dienstleistung notwendigen Maß. Kopien oder Duplikate dieser Daten werden ohne Wissen des Auftraggebers nicht erstellt.
(2) Der Aufragnehmer bestätigt die Einhaltung seiner Pflichten gemäß DSGVO und analog dazu die Beachtung der Bestimmungen gemäß KDG. Zu den Pflichten gehört u.a. das Führen eines Verzeichnisses aller Verarbeitungstätigkeiten im Unternehmen.
(3) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber jederzeit berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang - nach rechtzeitiger Ankündigung auch vor Ort zu kontrollieren oder durch vom Auftraggeber bestellte Prüfer kontrollieren zu lassen. Alle für solche Kontrollen relevanten Informationen sind vom Auftragnehmer bereitzustellen.
(4) Nicht mehr benötigte Unterlagen und Dateien mit personenbezogenen Daten des Auftraggebers werden vom Auftragnehmer zeitnah datenschutzkonform gelöscht / vernichtet.
(5) Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder auf dessen Weisung hin datenschutzkonform zu löschen.
(6) Für die Datensicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen.
(7) Falls der Auftragnehmer für bestimmte Arbeiten im Rahmen der Auftragserfüllung Subunternehmer einsetzen muss, hat er diese mit der gebotenen Sorgfalt auszuwählen und insbesondere darauf zu achten, dass

- der Subunternehmer eventuellen Verpflichtungen nach der DSGVO ausreichend nachgekommen ist
- der Subunternehmer bei der Arbeit für den Auftragnehmer nur Personal einsetzt, dass gemäß Artikel 39 DSGVO auf das Datengeheimnis verpflichtet wurde
- die Vertragsgestaltung den Vorgaben des Artikel 28 DSGVO entspricht.

Jedweder Einsatz oder Wechsel eines Subunternehmers ist im Vorfeld vom Auftraggeber schriftlich genehmigen zu lassen. Eine Liste der derzeit eingesetzten Subunternehmer findet sich in Anlage 2.
(8) Der Auftragnehmer bestätigt, dass er selbst die Auflagen gemäß DSGVO hinreichend erfüllt und einen Beauftragten für den Datenschutz bestellt hat.

Für den Datenschutz ist bestellt:

Herr Volker Atzpodin
ASB Informationstechnik GmbH
Bahnhofstraße 90
45711 Datteln
Telefon: +49 2363 605-876
Fax: +49 2363 605-859
E-Mail: v.atzpodin@asbinfo.de

(9) Der Auftragnehmer unterstützt den Auftraggeber darin, seiner Pflicht zur Bearbeitung von Anfragen Betroffener gemäß Kapitel III DSGVO nachzukommen. Ebenso unterstützt der Auftragnehmer auch bei notwendigen Aktivitäten gemäß Artikel 32-36 DSGVO. Anfragen oder Beschwerden Betroffener wird der Auftragnehmer unverzüglich an den Auftraggeber weiterleiten.
(10) Verstoßen Auftragsleistungen aus Sicht des Auftragnehmers gegen Datenschutzbestimmungen, so ist der Auftraggeber hierüber unverzüglich zu informieren. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.
(11) Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen oder Subunternehmer Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.
(12) Ebenso wird der Auftragnehmer den Auftraggeber unverzüglich unterrichten, wenn bei ihm Kontrollmaßnahmen oder Ermittlungen der Aufsichtsbehörden durchgeführt werden.
(13) Der Auftragnehmer hat auf Anfragen an der Erstellung und Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten des Auftraggebers mitzuwirken.

§ 4 Datengeheimnis

(1) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter gemäß Artikel 39 DSGVO und § 5 KDG mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut gemacht und auf das Datengeheimnis verpflichtet hat. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.
(2) Auskünfte darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

§ 5 Datensicherheit

(1) Die Maßnahmen zur technisch-organisatorischen Sicherheit gemäß Artikel 32 DSGVO sind in Anlage 1 beschrieben und bilden einen verbindlichen Bestandteil dieser Vereinbarung. Der Auftraggeber hat sich von der Angemessenheit der getroffenen Maßnahmen überzeugt und wird das regelmäßig tun.
(2) Der Auftragnehmer wird die technisch-organisatorischen Sicherheitsmaßnahmen kontinuierlich überprüfen und gegebenenfalls dem aktuellen Stand der Entwicklung anpassen.

§ 6 Vertragsdauer

Die Laufzeit dieser Vereinbarung entspricht der Laufzeit der Verträge im Rahmen der Softwarepflege und Problemanalyse zwischen Auftraggeber und Auftragnehmer. Sie tritt mit der Unterzeichnung beider Parteien in Kraft. Der Auftraggeber kann diese Vereinbarung ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen diese Vereinbarung vorliegt oder wenn der Auftragnehmer vereinbarungsgemäße Kontrollen durch den Auftraggeber ganz oder teilweise verhindert.

§ 7 Haftung

(1) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung schuldhaft verursachen.
(2) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach der DSGVO oder anderen Datenschutzvorschriften unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber dem Betroffenen verantwortlich. Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten. Gesetzliche Haftungsregelungen bleiben davon unberührt.
(3) Im Übrigen gilt Artikel 82 DSGVO.

§ 8 Sonstiges

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
(2) Für Nebenabreden ist die Schriftform erforderlich.
(3) Es werden keine Daten gemäß DSGVO Artikel 9 verarbeitet.

§ 9 Wirksamkeit der Vereinbarung

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. „Sollten Bestimmungen dieses Vertrages unwirksam sein oder werden oder sollte sich in diesem Vertrag eine Lücke herausstellen, so wird infolge dessen die Gültigkeit der übrigen Bestimmungen des Vertrages nicht berührt. Anstelle der unwirksamen Bestimmungen oder zur Ausfüllung der Lücke ist eine angemessene Regelung zu vereinbaren, die dem am nächsten kommen soll, was die Vertragsschließenden gewollt haben oder nach Sinn und Zweck des Vertrages gewollt haben würden, soweit sie den Punkt beachtet hätten."

Dinslaken, den

RIB IMS GmbH

Unterschrift Auftragnehmer

Unterschrift Auftraggeber

Anlage 1

Technische und organisatorische Maßnahmen gemäß Artikel 32 Abs. 1 DSGVO

1. Gewährleistung der Vertraulichkeit

- Zutrittskontrolle mittels Schlüssel-und Sicherheitscode.
- Schlüsselausgaben werden dokumentiert.
- Besucher werden Empfangen und Begleitet.
- Die Zutrittsberechtigungen sind auf einen Personenkreis bzw. einzelne Mitarbeiter beschränkt.
- Zugänge werden mit Kennwörtern geschützt (min. 8 Zeichen, Komplexität, Austausch alle 6 Monate).
- Protokollierung von Systemzugriffen, sofern möglich und sinnvoll.
- Zugang zu Systemen erfolgt mittels Benutzername und Passwort.
- Der VPN Zugriff in das Firmennetzwerk erfordert eine Zwei-Faktor Authentifizierung (Token).
- Datenträger werden in verschließbaren Schränken aufbewahrt und die Herausgabe dokumentiert.
- Zugriffsmöglichkeiten werden Abteilungs-oder Mitarbeiterabhängig gesteuert und je nach zugrundeliegendem IT-System auf Dateien, Datensätze, Datenfelder etc. eingeschränkt.
- Die Weitergabe von Daten unterliegt Regeln:
  - Datenträger werden physisch zerstört oder nach aktueller Empfehlung des BSI überschrieben.
  - Papier wird in einem Reißwolf oder bei größeren Mengen durch eine Fremdfirma entsorgt (DIN 66399).
  - Datenträger, Notebooks und andere mobile Geräte werden mit aktuellen Verfahren verschlüsselt.
  - Datenübertragungen über das Internet finden verschlüsselt statt.
  - Projektabhängiger Einsatz gesicherter Kollaborationsplattformen (Sharepoint).
- Trennung von Produktiv- und Testumgebungen.
- Nutzung der Mandantenfähigkeit relevanter Anwendungen.
- Nach technischer Möglichkeit findet eine Pseudonymisierung bzw. Anonymisierung der Daten statt.

2. Gewährleistung der Integrität

- Protokollierung von eingegeben Daten und der weiteren Verarbeitung.
- Die Verarbeitung von Daten findet entsprechend Auftrag oder auf Weisung statt.

Festlegung der Weisungsbefugten und Empfänger.

3. Gewährleistung der Verfügbarkeit

- Regelmäßige Systemwartungen (Update, Patches, Prüfung von Protokollen).
- Tägliche Datensicherungen.
- Festplattenspiegelung.
- USV Anlagen / Überspannungsfilter.

Einsatz redundanter Hardware.

4. Gewährleistung der Belastbarkeit der Systeme

- Flächendeckender Einsatz eines Virenscanners.

Schutz des Unternehmensnetzwerkes mit einer Firewall (IPS, Webfilter etc.).

5. Wiederherstellung der Verfügbarkeit

- Es werden aktuelle Backups vorgehalten.
- Durch den Einsatz redundanter Systeme und den Abschluss von Serviceverträgen mit Hardwarelieferanten ist eine Wiederherstellung werktags von Montag bis Freitag innerhalb von 24 Std. sichergestellt.

6. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

- Regelmäßige Prüfung auf Updates der eingesetzten Software.
- Wöchentliche Prüfung der Hardwareprotokolle.
- Quartalsweiser USV Test.
- Wöchentliche Sichtung von Firewall Protokollen.
- Tägliche Kontrolle der Backups.
- Monitoring der Server- und Netzwerkinfrastruktur.
- Monitoring des Virenschutzes.
- Regelmäßige Überprüfung der eingesetzten IT Sicherheitsverfahren auf Aktualität (BSI Empfehlungen).
- Regelmäßige Überprüfungen der Zugriffsrechte der Mitarbeiter in den einzelnen Verfahren.

Regelmäßige Überprüfung der Verfahren auf Möglichkeiten zur Datenminimierung, Pseudonymisierung und Verschlüsselung.

Es liegen schriftlich vor:

☐ Organisationsanweisungen zu wichtigen, hier beschriebenen Maßnahmen
☐ Risikoanalyse ☐ Datenschutzkonzept
☐ Datensicherheitskonzept ☐ Richtlinie zum Mobilen Arbeiten und Homeoffice
☐ Richtlinie zum Mobilen Arbeiten und Homeoffice

Anlage 2

Liste der vom Auftragnehmer eingesetzten Subunternehmen

☐ Es werden keine Subunternehmen eingesetzt

☐ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Subunternehmen zu

Name der Firma	Adresse	Art der Dienstleitung