

Vereinbarung zur Auftragsverarbeitung

Zwischen

Firma/ Company

Straße/ Street Name

Hausnummer / House number

Postleitzahl / Postal code

Ort / City

Land / Country

- **Auftraggeber** -

und

der Kompetenz für Schienengebundene Verkehre GmbH, Ludwig-Erhard-Straße 55a, 04103 Leipzig,
vertreten durch die Geschäftsführung, ebenda

- **Auftragnehmer** -

§ 1 Beschreibung der Verarbeitung

1. Folgende Individualangaben hinsichtlich der Verarbeitung sind in **Anhang A** dieses Vertrages dargestellt:

- a. Der Gegenstand, Art, Zweck und die Geltungsdauer der Verarbeitung sowie die Art der zu verarbeitenden Daten und die Kategorien der Betroffenen.

Zusätzliche Angaben sind im Vertrag zur Nutzung der Software RZBneo® und dessen Anlage 1 (Allgemeine Nutzungsbedingungen (ANB) der Kompetenz für Schienengebundene Verkehre GmbH für die Nutzung der Software RZBneo® und optionaler Module) und Anlage 2 (Leistungsbeschreibung zum Produkt RZBneo® und optionale Module dargestellt.

(im Folgenden allumfänglich und der Einfachheit halber: „Hauptvertrag“)

§ 2 Ort der Datenverarbeitung

1. Die Verarbeitung der Daten findet ausschließlich in einem Mitgliedstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt.
2. Erfolgt die Verarbeitung von personenbezogenen Daten durch einen Unterauftragsverarbeiter im Rahmen eines Drittstaatentransfers i.S.v. Art. 44 ff. DSGVO, ist der Auftragnehmer als Datenexporteur verpflichtet, geeignete Garantien, d.h. insbesondere die Standardvertragsklauseln und gegebenenfalls erforderliche zusätzliche Maßnahmen zu vereinbaren.

§ 3 Ansprechpartner / Datenschutzbeauftragter

1. Die Ansprechpartner sowie Angaben zum Datenschutzkoordinator bzw. Datenschutzbeauftragten sind in **Anhang A** dargestellt.

2. Änderungen diesbezüglich wird der Auftragnehmer dem Auftraggeber unverzüglich mitteilen.

§ 4 Weisungsgebundenheit

1. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers verarbeiten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
2. Eine Ausnahme von der Weisungsgebundenheit gilt nur, sofern der Auftragnehmer gesetzlich zu einer abweichenden Verarbeitung verpflichtet ist. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, das betreffende Recht verbietet eine solche Mitteilung wegen eines wichtigen öffentlichen Interesses.
3. Soweit eine betroffene Person sich mit einer Berichtigungs-, Löschungs- oder sonstiger Aufforderung in Bezug auf ihn betreffende Daten unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Löschkonzept, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers sind unmittelbar durch den Auftragnehmer durchzuführen.
4. Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die Datenschutzgrundverordnung (DSGVO) oder gegen andere Datenschutzbestimmungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen bei dem Auftraggeber bestätigt oder geändert wird.
5. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich mindestens in Textform.

§ 5 Technische und organisatorische Maßnahmen

1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft der Auftragnehmer geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
2. Der Auftragnehmer stellt unter Maßgabe des obigen Absatzes dauerhafte Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Datenverarbeitung sicher. Bei einem physischen oder technischen Zwischenfall werden Verfügbarkeit der personenbezogenen Daten sowie der Zugriff zu ihnen rasch wiederherstellgestellt.
3. Die technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit sind in einem schriftlichen Datensicherheitskonzept des Auftragnehmers dargestellt. Das aktuelle Sicherheitskonzept des Auftragnehmers ergibt sich aus der **Anhang B** zu der vorliegenden Vereinbarung.
4. Der Auftragnehmer verpflichtet sich zur regelmäßigen Überprüfung, Bewertung und Evaluierung des Datensicherheitskonzepts auf Gültigkeit und Wirksamkeit. Das Verfahren der Überprüfung, Bewertung und Evaluierung findet jährlich statt. Die Überprüfung, Bewertung und Evaluierung findet anhand aktueller Testate, Berichte oder Berichtsauszüge eines Datenschutzbeauftragten oder durch eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI Grundschrift) statt. Näheres ergibt sich aus dem aktuellen Datensicherheitskonzept (Anhang B).
5. Der Auftragnehmer passt das Sicherheitskonzept der technischen und organisatorischen Weiterentwicklung an. Mehr als nur unwesentliche Änderungen des Sicherheitskonzepts sind dem Auftraggeber vor ihrer Umsetzung anzuzeigen und mit dieser abzustimmen.

6. Der Auftragnehmer führt zur Gewährleistung eines angemessenen Datenschutzniveaus notwendige personelle Maßnahmen durch. Diese sind insbesondere: sorgfältige Auswahl des Personals, Eingangs- sowie jährliche Folgeschulungen.

§ 6 Verpflichtung zu Vertraulichkeit und Verschwiegenheit; Informationspflichten über behördliche Maßnahmen

1. Der Auftragnehmer setzt bei der Durchführung des Hauptvertrags nur Beschäftigte ein, die zur Vertraulichkeit verpflichtet wurden bzw. einer gesetzlichen Verschwiegenheitspflicht unterliegen.
2. Der Auftragnehmer wird dem Auftraggeber über Kontrollhandlungen und –maßnahmen von Aufsichts- und Ermittlungsbehörden, soweit sich auf die für den Auftraggeber erbrachten Leistungen beziehen, unverzüglich mit, es sei denn eine solche Mitteilung ist aufgrund von Unions- oder deutschem Recht unzulässig.

§ 7 Unterauftragsverhältnisse

1. Der Auftraggeber stimmt zu, dass der Auftragnehmer Unterauftragnehmer bei der Verarbeitung der Daten des Verantwortlichen hinzuzieht. Vor Hinzuziehung oder Ersetzung der Unterauftragsverarbeiter informiert der Auftragnehmer den Auftraggeber zumindest in Textform unter konkreter Nennung des weiteren Auftragsverarbeiters, der vorgesehenen Tätigkeit und des Ortes der Datenverarbeitung. Der Auftraggeber kann gegen die Änderung innerhalb einer Frist von zwei Wochen ab Kenntnisnahme gegenüber dem Auftragnehmer zumindest in Textform aus wichtigem und nachzuweisendem, datenschutzrechtlichem Grund Einspruch erheben. Ein wichtiger Grund liegt in der Regel dann vor, wenn dem Auftraggeber Informationen über den Unterauftragnehmer vorliegen, welche zeigen, dass dieser datenschutzrechtliche Vorschriften nicht einhält und diese Informationen dem Auftragnehmer zumindest in Textform zukommen lässt. Erfolgt kein Einspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als erteilt. Sofern ein wichtiger datenschutzrechtlicher Grund vorliegt und diesem nicht einvernehmlich abgeholfen werden kann, unterbleibt die Hinzuziehung des Unterauftragnehmers.
2. Die vertraglichen Vereinbarungen zwischen dem Auftragnehmer und den Unterauftragsverarbeitern sind durch den Auftragnehmer so zu gestalten, dass sie den Vereinbarungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen. Die Parteien stimmen überein, dass diese Anforderung erfüllt ist, wenn der Vertrag ein diesem Vertrag entsprechendes Schutzniveau aufweist bzw. dem Unterauftragsverarbeiter die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegt sind.
3. Der Auftragnehmer stellt sicher, dass diese Unterauftragsverarbeiter die technischen und organisatorischen Maßnahmen dieser Vereinbarung so implementieren, dass die Datensicherheitsmaßnahmen nach dieser Vereinbarung vollumfänglich beachtet werden.
4. Der Auftraggeber stimmt der Beauftragung der in **Anhang A** dargestellten Unterauftragnehmer zu.
5. Der Auftraggeber ist berechtigt, vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

§ 8 Pflicht zur Unterstützung des Auftraggebers hinsichtlich der Rechte Betroffener

1. Der Auftragnehmer hat den Auftraggeber bei der Wahrung von Rechten Betroffener, insbesondere im Hinblick auf die Benachrichtigung, Auskunftserteilung, Berichtigung, Sperrung und Löschung zu unterstützen. Der Auftragnehmer hat eine Berichtigung, Löschung oder Sperrung von Daten, die der Betroffene von dem Auftraggeber rechtmäßig verlangt, im Benehmen mit dem Auftraggeber unverzüglich vorzunehmen.
2. Der Auftragnehmer hat von den durch ihn beauftragten Unterauftragnehmern eine rechtmäßig verlangte Berichtigung, Löschung und Sperrung dieser Daten vertraglich sicher zu stellen. Der Auftragnehmer hat dem Auftraggeber alle Auskünfte zu erteilen, die zur Erfüllung von

Auskunftspflichten gegenüber dem Betroffenen erforderlich sind, oder auf Weisung des Auftraggebers dem Betroffenen selbst Auskunft zu erteilen.

§ 9 Unterstützung bei der Erfüllung der Pflichten aus Art. 32 bis 36 DS-GVO

1. Der Auftragnehmer wird unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Auftraggeber bei der Einhaltung der in den Artikeln 32 und 36 DSGVO genannten Pflichten unterstützen. Hieraus ergeben sich für den Auftragnehmer unter anderem nachfolgende Pflichten.
2. Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine von dem Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:
 - a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 - b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
 - c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - d) eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

Auch wird der Auftragnehmer im Falle einer Verletzung des Schutzes personenbezogener Daten in Abstimmung mit dem Auftraggeber geeignete technische und organisatorische Maßnahmen treffen, um die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich zu machen, etwa durch Verschlüsselung, sowie mögliche nachfolgende Maßnahmen ergreifen, damit das Risiko für die Rechte und Freiheiten betroffener Personen aller Wahrscheinlichkeit nicht mehr besteht.

Der Auftragnehmer verpflichtet sich, den Auftraggeber im Rahmen ihrer Informationspflichten nach Artikel 34 DSGVO gegenüber dem Betroffenen zu unterstützen und ihr in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen.

3. Der Auftragnehmer wird laufend überprüfen, ob eine Form der Verarbeitung einer Datenschutz-Folgenabwägung gemäß Art. 35 DS-GVO bedarf. Jedenfalls vor der Verwendung einer neuen Technologie für die Verarbeitung von Daten wird der Auftragnehmer standardmäßig eine Aufstellung der für eine Datenschutz- Folgenabschätzung nach Art. 35 DSGVO erforderlichen Angaben erstellen und dem Auftraggeber zur Verfügung stellen. Der Auftragnehmer wird diese Aufstellung laufend aktualisieren.
4. Der Auftragnehmer wird den Auftraggeber bei der Durchführung einer Datenschutz-Folgenschatzung nach Art. 35 DSGVO unterstützen und notwendige Informationen bereitstellen.
5. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei Konsultation der Aufsichtsbehörden nach Art. 36 DSGVO zu unterstützen. Seine eigenen Pflichten aus Art. 36 DS-GVO bleiben hiervon unberührt.

§ 10 Allgemeine Unterstützungspflichten

1. Die Parteien arbeiten hinsichtlich Anfragen von Aufsichtsbehörden zusammen. Soweit der Auftraggeber einer Kontrolle durch Aufsichts- und/oder Ermittlungsbehörden ausgesetzt ist, hat sie der Auftragnehmer nach besten Kräften zu unterstützen.

§ 11 „Home-Office“-Regelung

1. Der Auftragnehmer darf seinen Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten für den Auftraggeber beauftragt sind, die Verarbeitung von personenbezogenen Daten in Privatwohnungen („Home-Office“) erlauben.
2. Der Auftragnehmer hat sicherzustellen, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch im „Home-Office“ der Beschäftigten des Auftragnehmers gewährleistet ist.
3. Der Auftragnehmer trägt insbesondere Sorge dafür, dass bei einer Verarbeitung von personenbezogenen Daten im „Home-Office“ die Speicherorte so konfiguriert werden, dass eine lokale Speicherung von Daten auf IT-Systemen, die im „Home-Office“ verwendet werden, ausgeschlossen ist. Sollte dies nicht möglich sein, hat der Auftragnehmer Sorge dafür zu tragen, dass die lokale Speicherung ausschließlich verschlüsselt erfolgt und andere im Haushalt befindliche Personen keinen Zugriff auf diese Daten erhalten.
4. Der Auftragnehmer ist verpflichtet, Sorge dafür zu tragen, dass eine wirksame Kontrolle der Verarbeitung personenbezogener Daten im Auftrag im „Home-Office“ durch den Auftraggeber möglich ist. Dabei sind die Persönlichkeitsrechte der Beschäftigten sowie der weiteren im jeweiligen Haushalt lebenden Personen angemessen zu berücksichtigen.
5. Sofern auch bei Unterauftragnehmern Beschäftigte im „Home-Office“ eingesetzt werden sollen, gelten die Regelungen der Absätze 1 bis 4 entsprechend.

§ 12 Löschung und Rückgabe von personenbezogenen Daten

1. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber - spätestens mit Beendigung des Hauptvertrags - hat der Auftragnehmer sämtliche personenbezogene Daten, insbesondere Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse, Test- und Ausschussmaterial sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen und in den Besitz des Auftragnehmers gelangt sind, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Dies gilt nicht, sofern für den Auftragnehmer nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. In einem solchen Fall teilt der Auftragnehmer den Inhalt und die Grundlage der Verpflichtung mit.
2. Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Unterbeauftragten herbeizuführen, sofern nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten nicht besteht.
3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 13 Kontrollrechte des Auftraggebers

1. Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme vor Ort zu kontrollieren. Soweit nicht aus von dem Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers statt.
2. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen.
3. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger

Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) sowie eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erfolgen. Die Kosten für etwaige Nachweise, die nicht im direkten Zusammenhang mit der Auftragsverarbeitung stehen, trägt der Auftraggeber.

§ 14 Außerordentliche Kündigung

1. Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß gegen Bestimmungen dieser Vereinbarung vorliegt.
2. Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat. Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.
3. Der Auftragnehmer hat dem Auftraggeber alle Kosten zu erstatten, die diesem durch die verfrühte Beendigung des Hauptvertrages oder dieses Vertrages in Folge einer außerordentlichen Kündigung durch den Auftraggeber entstehen.

§ 15 Haftung

1. Es gelten die Bestimmungen des Art. 82 DSGVO.

§ 16 Sonstiges

1. Für Nebenabreden ist die Textform erforderlich.
2. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Ort, Datum

Ort, Datum

Unterschrift Auftragnehmer

Unterschrift Auftraggeber

Anhänge:

Anhang A – Beschreibung der Verarbeitung

Anhang B – Technische und organisatorische Maßnahmen