

Zusätzliche Vertragsbedingungen der Deutschen Bahn Aktiengesellschaft und der mit ihr verbundenen Unternehmen - nachstehend AG genannt - für die Benutzung von Datenverarbeitungsanlagen durch Dritte (ZVB-EDV)

Der Dritte muss nach Maßgabe des Architekten-/Ingenieurvertrages zur Erfüllung seiner Leistungen Daten an die EDV-Systeme des Auftraggebers (AG) übertragen (maskengesteuerte Online-Eingaben).

Management der Informationssicherheit:

Der Auftragnehmer hat in seinem Unternehmen geeignete Prozesse zur Gewährleistung der Informationssicherheit im Rahmen der Leistungserbringung etabliert und hält dieses während der gesamten Vertragslaufzeit aufrecht. Beispielsweise geschieht dies in Form eines wirksamen Informationssicherheitsmanagementsystems (ISMS).

1 Bereitstellen des Betriebssystems und systemnaher Software

Der AG stellt innerhalb seines Netzwerkes die Komponenten Datenbank, Betriebssystem und aktuelle Applikationen für Datenübertragungen auf Serverseite zur Verfügung.

2 Verfügbare Nutzerzeiten

Projektmanagementsystem iTWO, Datenbank Betra-Antragerstellung und Dokumentenmanagement-System (VRI DMS) DOXiS
Betriebsgeführte Zeiten Mo – Fr von 7:00 bis 18:00 Uhr,
Server-Verfügbarkeit Mo – Fr von 6:00 bis 22:00 Uhr (ausgenommen Wartungsfenster)
Projektkommunikationsplattform 24/7 (ausgenommen Wartungsfenster)

3 Datensicherung

Der AG übernimmt die Sicherung der Daten.

4 Störungsfälle

Bei ungeplanten Unterbrechungen der Anwendung erteilt der AG dem Dritten auf Anfrage Auskunft über die voraussichtliche Dauer der Unterbrechung.

5 Datenschutz

5.1 Sicherheit der Informationssysteme und IT-Zugriffe

- (1) Ein direkter oder verdeckter Zugriff auf operative Systeme, Netze, Programme oder Datenbestände des Auftraggebers oder der mit ihm verbundenen Unternehmen ist dem Auftragnehmer nur gestattet, wenn hierfür eine ausdrückliche, personenbezogene Zugriffsberechtigung in Textform durch den Auftraggeber erteilt wurde. Die Zugriffsberechtigungen sind auf die jeweils eingesetzten und ausdrücklich zugelassenen Mitarbeiter des Auftragnehmers bzw. seiner Nachunternehmer beschränkt. Eine Weitergabe der Zugriffsberechtigungen an Dritte ist unzulässig. Der Zugriff darf ausschließlich im Rahmen der vertraglich geschuldeten Leistungen erfolgen.
- (2) Sofern Nutzungsbestimmungen zum Anschluss oder zur Nutzung von Geräten an Datennetze des Auftraggebers bestehen, sind diese durch den Auftragnehmer verbindlich einzuhalten. Eine Verbindung zu den Datennetzen des Auftraggebers ohne Einhaltung dieser Vorgaben ist unzulässig. Die jeweils gültigen Nutzungsbestimmungen werden dem Auftragnehmer auf schriftliches Verlangen zur Verfügung gestellt.

- (3) Der Auftragnehmer verpflichtet sich zum sachgerechten Einsatz der von ihm eingesetzten IT- und OT-Systeme (z. B. Notebooks, mobile Endgeräte) innerhalb der Datennetze des Auftraggebers. Es dürfen ausschließlich Systeme eingesetzt werden, die dem jeweils aktuellen Stand der Technik entsprechen. Der Auftragnehmer stellt insbesondere sicher, dass geeignete Schutzmaßnahmen getroffen werden, um das Eindringen von Viren oder sonstigem schädlichen Code zu verhindern. Hierzu zählen insbesondere der Einsatz aktueller Virenschutzprogramme sowie die regelmäßige Durchführung von Sicherheitsupdates, Patches und Servicepacks.
- (4) Der Einsatz von Hacking-Tools, Sniffern oder vergleichbaren Werkzeugen ist unzulässig, sofern hierfür keine ausdrückliche Genehmigung des Auftraggebers vorliegt. Ebenso ist jede Netzkopplung der Datennetze des Auftraggebers mit anderen Datennetzen durch den Auftragnehmer unzulässig.
- (5) Nach Beendigung des Auftragsverhältnisses ist der Auftragnehmer verpflichtet, sämtliche im Zusammenhang mit dem Auftragsverhältnis stehenden Daten an allen primären und sekundären Standorten des Auftragnehmers sowie seiner Nachunternehmer unverzüglich, sicher und nachhaltig zu löschen, zu vernichten oder an den Auftraggeber zurückzugeben, soweit keine gesetzliche Aufbewahrungspflicht besteht. Der Auftragnehmer hat dies auf Verlangen des Auftraggebers in geeigneter Form nachzuweisen.
- (6) Der Auftraggeber ist berechtigt, Sperrungen, Überwachungen oder Unterbrechungen des Netzzugangs vorzunehmen, sofern dies aufgrund behördlicher Anordnungen, geltender Nutzungsbestimmungen oder zur Abwehr von Gefahren für die Betriebs- oder Informationssicherheit erforderlich ist.
- (7) Die vorstehenden Regelungen gelten vorbehaltlich abweichender oder ergänzender Vereinbarungen zum Umgang mit personenbezogenen Daten im Auftragsverhältnis.

5.2 Weiteres zum Thema Datenschutz

- (1) Für die Kontrolle des Datenzugriffs ist die Datenschutzsoftware des BKU-Systems eingesetzt. Für SAP gilt zusätzlich RACF; für die Betra-Antragerstellung gelten zusätzlich die Bedingungen des Workflow Betra-Antragerstellung; für DMS gelten die Regelungen der GBV.
- (2) Für die vom Dritten eingestellten Daten innerhalb von Datenbanken übernimmt der AG keine Gewähr für Integrität.
- (3) Der Dritte führt die Aufträge unter Beachtung der ihn verpflichtenden gesetzlichen Datenschutz- und Geheimhaltungsvorschriften durch.
- (4) Der Dritte darf Daten nur für die Durchführung des jeweiligen Auftrags verwenden. Eine Weitergabe ist untersagt. Der Dritte stellt sicher, dass diese Auflagen in gleicher Weise auch von beauftragten Nachunternehmern eingehalten werden. Der Einsatz solcher Nachunternehmer bedarf der vorherigen schriftlichen Zustimmung des AG.
- (5) Wenn der AG dem Dritten den Zugriff auf Dateien eröffnet, kann der AG verlangen, dass der Dritte den Inhalt der daraus verwendeten Daten offenlegt. Der AG ist darüber hinaus berechtigt, den Inhalt vom Dritten eingerichteter Dateien zu überprüfen.
- (6) Ein Anspruch des Dritten auf Zugriff auf andere als die für die Anwendungen benötigten Datenbanken besteht nicht. Der gewährte Zugriff zu Dateien kann jederzeit ohne Angabe eines Grundes vom AG widerrufen werden.
- (7) Sofern der Auftragnehmer eigene Endgeräte zur Erbringung der vereinbarten Dienstleistung einsetzt, verpflichtet er sich zur Einhaltung der nachstehend genannten Vorgaben des Auftraggebers. Als Endgerät im Sinne dieser Regelung wird jedes IT-Asset des Auftragnehmers verstanden, dass an IT-Applikationen sowie IT-Infrastruktur des Auftraggebers (kabelgebunden oder kabellos) angeschlossen oder zur Verarbeitung von Daten des Auftraggebers eingesetzt wird.

- Nur vom Auftragnehmer aktiv verwaltete Geräte dürfen verwendet werden.
- Die Nutzung von privaten Endgeräten zur Verbindung zu IT-Assets des DB-Konzerns ist untersagt, sofern nicht ausdrücklich vom Auftraggeber genehmigt.
- Die Endgeräte müssen nach dem jeweils aktuellen Stand der Technik abgesichert sein; dies bedeutet die Einrichtung eines Zugangsschutzes (Passwort oder PIN), Deaktivierung aller nicht benötigten Übertragungsprotokolle, Einsatz von Verschlüsselungsprotokollen bei Datenübertragung (bspw. WPA2 für Wi-Fi), Einsatz von Verschlüsselungstechnologien der gespeicherten Daten des Endgerätes.
- Der Auftragnehmer ist verantwortlich für den ordnungsgemäßen Umgang des Endgerätes sowie für den Schutz gegen Diebstahl; beim Einsatz des Endgerätes außerhalb der Lokationen des Auftraggebers darf das Endgerät nicht ungesichert bzw. unbeaufsichtigt bleiben.
- Der Auftragnehmer verpflichtet sich, den Verlust eines Endgerätes unverzüglich an die Verantwortlichen des Auftraggebers zu melden und dieses umgehend zu deaktivieren und zu sperren.
- Der Auftragnehmer stellt sicher, dass das Endgerät regelmäßig (mindestens einmal im Monat) auf Sicherheitsupdates geprüft und gemäß dem jeweils aktuellen Stand der Technik aktualisiert wird und weist dies auf Anfrage nach. Für die Datensicherung gelten die Anforderungen zur Datenverarbeitung.
- Der Einsatz von Hacking-Tools, Sniffen, etc. ist untersagt, sofern dies nicht ausdrücklich zugelassen ist.
- Der Auftragnehmer ist dafür verantwortlich, dass keine Netzkopplung der Datennetze des Auftraggebers und den mit diesem verbundenen Unternehmen mit anderen Datennetzen stattfindet.
- Nach Ende des Nutzungszeitraums ist die sichere und fachgerechte Entsorgung des Endgerätes durch den Auftragnehmer zu gewährleisten; dies beinhaltet das vollständige Entfernen aller Daten und/ oder das Entfernen von internen Speicherkarten.

6 Durchführen von Audits

Der AG behält sich vor in Bezug auf die getroffenen datenschutzrechtlichen Bestimmungen anlasslose/anlassbezogene Audits zur Überprüfung durchzuführen.

7 Nutzungsberechtigung

- (1) Jeder Anwender des Dritten benötigt eine eindeutige, personenbezogene Benutzerkennung (DB User). Diese beantragt er schriftlich unter Verwendung der entsprechenden Anträge bei der DB Systel GmbH.
- (2) Die beantragte Benutzerkennung wird bei Vorliegen der Voraussetzungen unverzüglich eingerichtet. Der Dritte wird vom AG über die erfolgte Einrichtung/Zuweisung der Benutzerkennung benachrichtigt. Die Weitergabe der persönlich zugeteilten Benutzerkennung an andere Personen ist strengstens untersagt.
- (3) Werden über einen Mitarbeiter des Dritten oder einen vom Dritten beauftragten Nachunternehmer Umstände bekannt, die auf ein Sicherheitsrisiko hindeuten, ist der AG berechtigt, über die zuständige Dienststelle des Bundes Auskünfte über diese Person einzuholen. Ergeben sich Sicherheitsbedenken, darf der AG jederzeit und mit sofortiger Wirkung die Benutzerkennung dieser Person zurückziehen.
- (4) Der Dritte stellt sicher, dass von ihm oder einem Nachunternehmer nicht unberechtigt auf das Netzwerk des AG zugegriffen wird. Der AG hat das Recht, bei unberechtigten Zugriffsversuchen die Anwendungen zu unterbrechen.
- (5) Bei missbräuchlicher Netzwerkanwendung kann der AG dem Dritten den Vertrag aus wichtigem Grund mit sofortiger Wirkung kündigen.
- (6) Für die Nutzung der Anwendung „Betra-Antragerstellung Datenbank“ ist zusätzlich zur personenbezogenen Benutzerkennung (DB User) erforderlich. Diese ist ebenfalls schriftlich unter Verwendung der entsprechenden Anträge bei der DB Systel GmbH zu beantragen. Auch für diese Benutzerkennung gelten die Regularien gemäß Punkt 7 (1-6).
- (7) Für die Nutzung der Anwendung VRI DMS ist zusätzlich zur personenbezogenen Benutzerkennung eine personenbezogene Benutzerkennung VRI DMS erforderlich. Diese ist ebenfalls schriftlich unter Verwendung der entsprechenden Anträge bei der DB Systel GmbH zu beantragen. Auch für diese Benutzerkennung gelten die Regularien gemäß Punkt 7 (1-6).

8 Löschung von Daten

Der Auftragnehmer gewährleistet, sämtliche im Zusammenhang mit dem Auftragsverhältnis stehenden Daten an allen Standorten des Auftragnehmers und seiner Nachunternehmer bei Beendigung des Vertrags unverzüglich und derart zu löschen und zu vernichten, so dass sie nicht wiederhergestellt werden können. Ausnahmen bestehen nur bei Daten, soweit und solange (a) der Auftragnehmer zu deren Aufbewahrung gesetzlich verpflichtet ist, (b) diese der administrativen Abwicklung des Vertrags dienen oder (c) dies vertraglich geregelt wurde. Der Auftragnehmer weist dies auf Verlangen des Auftraggebers nach. Dem Auftragnehmer steht kein Zurückbehaltungsrecht an den Daten zu.

9 Vergütungsregelung

(1) VDS-Zugang

Der Dritte schließt mit der

DB Systel GmbH
Jürgen Ponto Platz1
60326 Frankfurt/M.

einen Vertrag über den VDS (Produkt Enterprise VDS) Zugang zur Anbindung an das DB AG Netzwerk. Dieser Zugang ermöglicht den Zugriff auf die DB AG Verfahren wie z. B. Betra-Antragerstellung Datenbank usw. und das VRI DMS (DOXiS über VDS)

- Die Kosten für den Anschluss trägt der Dritte.
- Die monatlichen Zugangskosten trägt der Dritte. Die verschiedenen Produkte und Preise sind bei der DB Systel GmbH zu erfragen.
- Die Kosten für die Benutzung der Datendienste zum Einwahlknoten trägt der Dritte.
- Die Kosten für die erforderliche Einwahlsoftware (siehe Empfehlungen der DB Systel GmbH) am Client trägt der Dritte.
- Für die Nutzung der Datenbank Betra-Antragerstellung gelten die Regelungen in den "Besondere Bedingungen zur Nutzung Betra-Antragerstellung Datenbank".
- Für die Nutzung von VRI DMS fallen Kosten für RAS/RAC VPN, VDS und DOXiS an. Die Preise sind bei der DB Systel GmbH zu erfragen.

(2) System

1. iTWO-System

Die Anwendung des Systems iTWO durch Dritte ist lizenzpflichtig. Die Lizenzen muss der Dritte bei folgender Firma erwerben:

RIB Software GmbH

Vaihinger Straße 151
70567 Stuttgart
Tel: +49 711 7873-0
Fax: +49 711 7873-88204
info@rib-software.com

Die Einstellung des Users in iTWO erfolgt ausschließlich durch die beim Auftraggeber zuständige Stelle, d. h. der Dritte übergibt den ausgefüllten Userantrag seinem Auftraggeber auf Seiten der DB AG. Alles weitere veranlasst der Auftraggeber. Den Userantrag können Sie unter folgendem Link downloaden (iTWO-Antrag zum Download):

[https://dbsw.sharepoint.com/sites/bwpss/SitePages/Nav%20\(Confluence\)/iTWO%20Allgemein/iTWO%20Berechtigungen%20und%20Antr%C3%A4ge/Externe%20Mitarbeiter.aspx](https://dbsw.sharepoint.com/sites/bwpss/SitePages/Nav%20(Confluence)/iTWO%20Allgemein/iTWO%20Berechtigungen%20und%20Antr%C3%A4ge/Externe%20Mitarbeiter.aspx)

2. Projektkommunikationsplattform (PKP)

Die Anwendung des Systems Projektkommunikationsplattform durch Dritte ist lizenzpflichtig. Die Lizenzen muss der Dritte bei folgender Firma erwerben:

thinkproject Deutschland GmbH

Mühlendorfstr. 8
81671 München
Tel: +49 89 930839302

Die Einstellung des Users erfolgt durch thinkproject. Hierzu müssen jedoch einige Voraussetzungen (HR-Antrag, Antrag in PKP) geschaffen werden. Die konkrete Vorgehensweise entnehmen Sie bitte den folgenden Link:

<https://www1.deutschebahn.com/sus-infoplattform/start/baustandards>

(3) Ressourcen

Lizenzgebühren für die nachstehend aufgeführten Regelwerke und Kataloge des AG fallen für den Dritten nicht an. Entsprechende Druckstücke sind käuflich zu erwerben.

1. Kostenermittlungsbuch (KEB)

Artikel 80821

Das KEB dient der Kostenplanung. Es enthält die Module Kostengruppenkatalog (KGK), Artikel 808.0211, und Kostenkennwertekatalog (KKK), Artikel 808.0212. Die Buchform der jeweils neuesten Ausgabe beschafft sich der Dritte bei der

DB InfraGO AG

Medien & Kommunikation

Griesbachstr. 7

76185 Karlsruhe

E-Mail: auftraege.zu.technischen.regeln@deutschebahn.com

2. Standardleistungsbuch (STLB) und Standardleistungskatalog (STLK)

Die Standardleistungsbücher und der Standardleistungskatalog sind im Managementsystem iTWO hinterlegt. Anpassungen der STLB werden durch die Geschäftlichen Mitteilungen der DB AG bekannt gegeben.

(4) Externe Programme

1. STLB-Bau Dynamische BauDaten

Wendet der AN andere DB-Systeme zur Erstellung oder Bearbeitung von Leistungsverzeichnissen das STLB-Bau an, setzt dies eine Lizenz der aktuellen STLB-Bau-Version beim AN voraus.

2. REB

Wendet der Dritte zur Erfüllung seines Vertrages die REB (Regelungen für die elektronische Bauabrechnung) und deren Programme an, setzt dies eine Lizenz des AN voraus.

10 DWS (Digitale Weichenskizze)

(1) Die Punkte 1-8 gelten nicht für die Anwendung des Systems DWS.

(2) Die Anwendung des Systems DWS durch Dritte ist lizenzpflichtig. Die Lizenzen muss der Dritte bei folgender Firma erwerben:

IVE – DWS-Team

Ingenieurgesellschaft für Verkehrs- und Eisenbahnwesen mbH

Consulting Company for Traffic and Railway Engineering Ltd.

Vahrenwalder Platz 3

30165 Hannover

Phone: +49/(0)511/984228-15 oder /or +49/(0)511/984228-10

Fax: +49/(0)511/984228-29

Web: www.ivembh.de

11 eBTB VRI (elektronisches Bautagebuch Vorstandsbereich Infrastruktur)

- (1) Die Punkte 1 - 8 gelten nicht für die Anwendung eBTB VRI.
- (2) Die Anwendung durch Dritte ist lizenzpflichtig. Die Lizenzen muss der Dritte erwerben. Die Kosten sind durch den Dritten zu tragen.
- (3) Das Bestellformular für den Zugang/Lizenz eBTB VRI ist beim Auftraggeber abzufordern. Das ausgefüllte Formular (einschl. des benannten Paten des Konzerns) ist an die

DB Systel GmbH
T.IV D-T-204
Jürgen-Ponto-Platz 1
60329 Frankfurt
zu senden.

12 SEMYOU PCP (sem.PCP)

- (1) Die Punkte 1 - 8 gelten nicht für die Anwendung eBTB VRI.
- (2) Die Anwendung durch Dritte ist lizenzpflichtig und vor Erteilung einer Lizenz ist eine Teilnahme an einer 2stündigen Schulung erforderlich. Die Kosten für die Lizenz und Schulung werden vom AG getragen.
- (3) Die Lizenz muss der Dritte beim Projektleiter beantragen. Das Bestellformular für den Zugang/Lizenz SEMYOU PCP ist beim Auftraggeber abzufordern.

