Ergänzende Vertragsbedingungen

der Deutschen Bahn AG (DB AG) und der mit ihr verbundenen Unternehmen zu Anforderungen an die Informationssicherheit (EVB Informationssicherheit)

– Ausgabe 01.11.2026 –

1. Allgemeines

1.1 Der Auftragnehmer liefert dem Auftraggeber durch Informationstechnologie unterstützte Dienstleistungen bzw. IT (Information Technology)- oder OT (Operational Technology)-Assets bzw. Produkte, die im Vertrag näher spezifiziert werden.

1.2 Diese EVB regeln ergänzend Anforderungen an die Informationssicherheit, die vom Auftragnehmer zu erfüllen sind.

1.3 Der Auftragnehmer stellt die vertragsgegenständlichen Leistungen, soweit es sich um „Produkte mit digitalen Elementen“ handelt, ab dem 11.12.2027 unter Einhaltung der jeweils anwendbaren Anforderungen der Verordnung (EU) 2024/2847 (Cyber Resilience Act – CRA) bereit. Sonstige rechtliche Vorgaben sowie weitergehende Anforderungen in diesen EVB bleiben unberührt.

1.4 Die vom Vertrag abgedeckten Informationen und IT/OT-Assets können einem definierten Schutzbedarf (normal, hoch, sehr hoch) und gegebenenfalls speziellen gesetzlichen Anforderungen (z. B. der Gesetzgebung zu Kritischen Infrastrukturen) unterliegen. Hieraus leitet sich die konkrete Ausgestaltung der Maßnahmen zur Informationssicherheit ab. Der Schutzbedarf selbst sowie Details zu Maßnahmen sind, wenn zutreffend, im Vertrag dokumentiert. Ist der Schutzbedarf nicht angegeben bzw. sind keine weitergehenden Informationssicherheitsanforderungen im Vertrag definiert, gelten die Anforderungen für Schutzbedarf ‚normal‘ als vereinbart.

1.5 Soweit ein Audit (gemäß Ziffer 3.2 Audit) nachweislich aus berufsrechtlichen Gründen nicht wie vom Auftraggeber geplant durchgeführt werden kann, informiert der Auftragnehmer den Auftraggeber zeitnah über diese Gründe. Die Parteien stimmen dann einen modifizierten Auditplan ab. Dabei werden sowohl das für den Auftragnehmer geltende Berufsrecht als auch die Interessen des Auftraggebers berücksichtigt.

1.6 Dem Auftragnehmer durch die Umsetzung der Anforderungen dieser ergänzenden Vertragsbedingungen und eventueller Anhänge entstehenden Aufwände sind mit der vereinbarten Vergütung abgegolten. Ausnahmen hiervon sind in Form einer Vertragsergänzung zu vereinbaren. Die Umsetzung gesetzlicher Anforderungen ist hiervon ausgeschlossen.

1.7 Verstößt der Auftragnehmer gegen die Verpflichtungen aus den Ziffern 2.2.a), 2.4, 2.7 und 3.1 dieser ergänzenden Vertragsbedingung, hat er an den Auftraggeber je Verstoß eine Vertragsstrafe in Höhe von 2% der geschuldeten Vergütung aus dem jeweils betroffenen (Einzel-)Vertrag zu zahlen, es sei denn, der Verstoß ist nicht vom Auftragnehmer zu vertreten. Die Geltendmachung eines Schadenersatzes durch den Auftraggeber infolge derselben Pflichtverletzung bleibt von der Vertragsstrafe unberührt, wobei in diesem Fall eine verwirkte Vertragsstrafe auf diesen Schadenersatz angerechnet wird.

Die auf Grundlage dieser EVB Informationssicherheit geltend gemachten Vertragsstrafen belaufen sich auf maximal 5% der geschuldeten Vergütung aus dem jeweils betroffenen (Einzel-)Vertrag.

2. Anforderungen an die Informationssicherheit

2.1 Management der Informationssicherheit

Der Auftragnehmer hat in seinem Unternehmen geeignete Prozesse zur Sicherstellung der Informationssicherheit etabliert. Diese decken den gesamten für die Vertragserfüllung relevanten Lebenszyklus der gelieferten IT/OT-Assets, Produkte und Leistungen ab. Er hält diese Prozesse während der gesam-

ten Vertragslaufzeit aufrecht, beispielsweise durch ein wirksames Informationssicherheitsmanagementsystem (ISMS). Die Informationssicherheitsprozesse decken mindestens die in diesen EVB (inkl. Anhänge) beschriebenen Informationssicherheitsanforderungen ab.

2.2 Ansprechpartner zur Informationssicherheit

a) Koordinator Informationssicherheit

Der Auftragnehmer muss dem Auftraggeber mit Vertragsunterzeichnung für alle Aspekte rund um Informationssicherheit einen sachkundigen, verantwortlichen Ansprechpartner (z. B. Informationssicherheitsbeauftragten, IT-Sicherheitsmanager bzw. Chief Information Security Officer) benennen, der gegenüber dem Auftraggeber auskunftsfähig und auskunftsberechtigt ist.

b) Ansprechpartner zu vertragsspezifischen Themen der Informationssicherheit

Der Auftragnehmer benennt die zuständige Stelle oder eine Funktion zur vertraglichen Regel- und Notfallkommunikation, zu Themen der Informationssicherheit sowie zur Meldung identifizierter Schwachstellen. Die Stelle steht dem Auftraggeber zu den im Vertrag geregelten Fristen zur Verfügung. Im Notfall hat der Ansprechpartner Zugriff auf alle notwendigen Daten des Auftragnehmers (z. B. Produkt Monitoring, Zugriffs- und Konfigurationsdaten) und stellt bei der Notfallbewältigung die Schnittstelle zum Auftraggeber dar.

Bei Wechsel eines Ansprechpartners informiert der Auftragnehmer den Auftraggeber unverzüglich.

2.3 Personelle Sicherheitsanforderungen

Für die im Rahmen der Leistungserbringung eingesetzten Mitarbeitenden des Auftragnehmers sowie sonstige beauftragte Dritte (einschließlich Nachunternehmer) und deren Mitarbeitende gelten besondere Anforderungen an deren persönliche Zuverlässigkeit und Integrität.

Zur Sicherstellung dieser Anforderungen behält sich der Auftraggeber die Überprüfung der betroffenen Mitarbeitenden durch zusätzliche Prüf- und Auskunftsverfahren (sog. „Background Checks“) vor. Der genaue Umfang der Prüf- und Auskunftsverfahren orientiert sich an den einschlägigen regulatorischen und normativen Anforderungen zur personellen Sicherheit, insbesondere den Vorgaben des BSIG, den hierzu veröffentlichten Konkretisierungen des BSI sowie den Anforderungen des KRITIS-Dachgesetzes. Der Auftraggeber behält sich vor, Mitarbeitende erst nach erfolgreicher Überprüfung einzusetzen.

2.4 Qualifiziertes Personal

Der Auftragnehmer stellt sicher, dass das von ihm eingesetzte Personal die zur Auftragserbringung notwendige Qualifikation und Awareness hinsichtlich der Anforderungen zur Informationssicherheit besitzt und regelmäßig aktualisiert und weist dies dem Auftraggeber auf Anfrage – maximal einmal pro Jahr – nach.

2.5 Verpflichtung Nachunternehmer

Der Auftragnehmer gewährleistet, dass seine im Rahmen der Leistungserbringung eingesetzten Nachunternehmer und deren Nachunternehmer die Anforderungen aus diesem Vertrag oder die Anforderungen eines relevanten Informationssicherheitsrahmenwerks bzw. -norm entsprechen, z.B. der DIN EN ISO/IEC 27001. Er stellt entsprechende Nachweise auf Anforderung des Auftraggebers zur Verfügung.

Lieferanten des Auftragnehmers, die nur physische Produkte ohne digitale Elemente beistellen, sind keine Nachunternehmer im Sinne dieser Anforderung.

2.6 Verschlüsselung

Der Auftragnehmer gewährleistet, dass Informationen des Auftraggebers der Klassifizierungen „DB Intern“, „DB Vertraulich“ und „DB Streng Vertraulich“ bei elektronischer Übertragung grundsätzlich durch geeignete Transportverschlüsselung und bei Speicherung durch angemessene technische und organisatorische Maßnahmen nach dem Stand der Technik geschützt werden. Werden kryptographische Maßnahmen während der Vertragslaufzeit unsicher, sind diese nach Absprache zu ersetzen. Die Kostenübernahme hierzu wird einvernehmlich zwischen Auftraggeber und Auftragnehmer geregelt.

2.7 Rechtsräume Speicherung / Verarbeitung

Der Auftragnehmer verpflichtet sich, alle Länder, in denen Daten des Auftraggebers verarbeitet oder gespeichert sind zu benennen. Enthält die Leistungsbeschreibung darüberhinausgehende Anforderungen an Speicher- und Verarbeitungsorte, sind diese durch den Auftragnehmer zu bestätigen. Erfolgt die Speicherung nicht in den Systemen des Auftragnehmers, ist dies dem Auftraggeber separat anzuzeigen.

Der Auftragnehmer sichert zu, dass die benannten Speicher- und Verarbeitungsorte nicht verlassen werden. Umzüge innerhalb der EU sind hiervon ausgenommen, müssen dem Auftraggeber aber unverzüglich in Textform mitgeteilt werden.

2.8 Meldung Informationssicherheitsvorfälle

Der Auftragnehmer verpflichtet sich, den Auftraggeber über alle Informationssicherheitsvorfälle sowie Datenschutzverletzungen gemäß Art. 33 DSGVO zu informieren, die im Umfeld des Auftragnehmers oder eines seiner Nachunternehmer auftreten und Auswirkungen auf seine unmittelbare oder mittelbare Leistungserbringung für den Auftraggeber haben. Sofern der Informationssicherheitsvorfall unmittelbar Daten und/oder Assets des Auftraggebers und der mit diesem verbundenen Unternehmen betrifft, muss die Erstmeldung unverzüglich, spätestens aber 24h nach Kenntniserlangung des Sicherheitsvorfalls erfolgen, eine detaillierte Meldung einschließlich Auswirkungsanalyse spätestens nach 72h.

Die Meldung muss mindestens folgende Inhalte haben:

- Zeitpunkte des Vorfalls und der Vorfallserkennung
- Betroffene Systeme und Daten
- Ergriffene Maßnahmen
- Ersteinschätzung der Schwere / Kritikalität / rechtliche Relevanz

Vertragsspezifische Inhalte der Meldung werden innerhalb von acht Wochen nach Vertragsabschluss einvernehmlich in Textform vereinbart, spätestens jedoch vor Leistungsbeginn bzw. vor Lieferung des Produkts.

Die Meldungen erfolgen an ‚security-issues@deutschebahn.com' sowie die hierzu im Vertrag vereinbarten Kontakte.

Soweit Nachunternehmer und/oder Dienstleister eingesetzt werden, stellt der Auftragnehmer sicher, dass er gleichwohl die genannten Meldefristen einhalten kann.

2.9 Behandlung Informationssicherheitsvorfälle

Im Falle eines für den Auftraggeber relevanten Informationssicherheitsvorfalls (s. §2.8 dieser EVB) hat der Auftragnehmer neben der Information des Auftraggebers unverzüglich alle notwendigen Maßnahmen zu ergreifen, um die gebotene Sicherheit wiederherzustellen. Sofern hierfür ein konzertiertes Vorgehen mit dem Auftraggeber erforderlich ist, wird der Auftragnehmer sich mit detailliertem Maßnahmenkatalog an den Auftraggeber wenden und sich mit diesem abstimmen. Ist zur Bearbeitung der Maßnahmen die Unterstützung durch den Auftraggeber oder von ihm verbundener Unternehmen und / oder beauftragte Dritte notwendig, gewährt der Auftragnehmer diesen im Rahmen einer entsprechenden Vertraulichkeitsvereinbarung Zugang zu allen notwendigen Informationen, Systemen und Betriebsstätten.

2.10 Kontrolle des Zugangs

Ein direkter oder verdeckter Zugang zu den Informationssystemen (u.a. operative Systeme, Netze, Anwendungen, Datenbestände) des Auftraggebers und der mit diesem verbundenen Unternehmen ist dem Auftragnehmer nur dann gestattet, wenn er vom Auftraggeber eine ausdrückliche, dokumentierte Zugangsberechtigung erhalten hat. Diese ist auf die eingesetzten und ausdrücklich zugelassenen Mitarbeitenden des Auftragnehmers bzw. seiner Nachunternehmer beschränkt. Die Weitergabe der Zugangsberechtigung an Dritte ist untersagt. Eine erteilte Zugangsberechtigung darf ausschließlich im Rahmen der vertraglich vereinbarten Leistungen genutzt werden. Fällt die Notwendigkeit einer Zugangsberechtigung weg (z. B. bei Weggang eines Mitarbeitenden), unterrichtet der Auftragnehmer den Auftraggeber unverzüglich.

3. Bewertung der Informationssicherheit beim Auftragnehmer

3.1 Bewertung der Sicherheitsorganisation

Der Auftragnehmer hat dem Auftraggeber auf Anfrage Informationen über seine Informationssicherheitsorganisation offenzulegen und geeignete Nachweise mit Bezug zur konkreten Leistung bereitzustellen, auf deren Grundlage der Auftraggeber eine Bewertung der Informationssicherheit vornehmen kann. Dies können z. B. ein Statusbericht zum ISMS (eine Vorlage kann auf Anfrage zur Verfügung gestellt werden), ein Management Summary zur Sicherheitsorganisation im Anwendungsbereich der Leistung, Berichte aus einem bestehenden Informationssicherheitsmanagementsystem, ein DIN EN ISO/IEC 27001-Zertifikat einschließlich detaillierter Beschreibung des Anwendungsbereichs, der Erklä-

rung der Anwendbarkeit (Statement of Applicability (SoA)) und des DIN EN ISO/IEC 27001-Prüfberichts, ein VdS-10000-Zertifikat oder äquivalente Nachweise wie aktuelle Auditergebnisse im Anwendungsbereich der Leistung sein.

3.2 Audit

Der Auftragnehmer stimmt zu, dass der Auftraggeber oder ein von ihm beauftragter Dritter den Auftragnehmer während der Laufzeit des Vertrages in Bezug auf dessen Informationssicherheit und Einhaltung datenschutzrechtlicher Bestimmungen auditieren darf. Prüfgrundlage der Informationssicherheits-Audits ist die DIN EN ISO/IEC 27001 sowie der Stand der Technik. Geprüft wird die angemessene Umsetzung der vereinbarten Informationssicherheitsanforderungen und die Wirksamkeit der Informationssicherheitsorganisation bezogen auf den Auftrag. Basis der datenschutzrechtlichen Audits sind die DSGVO sowie das BDSG. Details zur Auditdurchführung, Aufwänden und eventuellen Folgemaßnahmen sind im Weiteren beschrieben.

a) Anlasslose Audits

Der Auftraggeber kündigt ein anlassloses Audit spätestens sechs Wochen vor dessen Durchführung an. Der Auftragnehmer stellt rechtzeitig (i. d. R. spätestens drei Wochen vor Durchführungstermin) die benötigten Unterlagen (z. B. Managementberichte, Berichte aus dem ISMS, betriebliche Unterlagen wie z. B. Konfigurations- und Berechtigungsdaten) zur Verfügung und kommt seinen Mitwirkungspflichten (z. B. Bereitstellen von Zugängen, Erteilung der notwendigen Zugriffsrechte) im Rahmen des Audits nach. Die Durchführung der Audits erfolgt zu den üblichen Geschäftszeiten. Der Auftraggeber stellt dem Auftragnehmer die Ergebnisse des Audits in Berichtsform zur Verfügung. Vom Auftragnehmer eingereichte Prüfberichte unabhängiger Dritter wie z.B. eine ISO27001- oder TISAX-Zertifizierung, ein ISAE3402- oder SOC2-Report, welche jeweils die zu erbringende Leistung abdecken, können nach Ermessen des Auftraggebers die Durchführung des Audits beschleunigen oder die Notwendigkeit erübrigen.

b) Anlassbezogene Audits

Der Auftraggeber hat das Recht, im Falle eines schweren Informationssicherheitsvorfalls oder wiederholten Verstößen gegen diese Ergänzende Vertragsbedingung anlassbezogen ein Audit durchzuführen, sofern der Auftraggeber von dem Vorfall betroffen ist. Die Audits können in Abhängigkeit von der Schwere des Anlasses kurzfristig erfolgen.

c) Maßnahmen zur Behebung von Nichtkonformitäten

Werden durch ein Audit Schwachstellen, Nichtkonformitäten oder Datenschutzverletzungen seitens des Auftragnehmers festgestellt, sind diese durch den Auftragnehmer zeitnah zu beheben. Auftraggeber und Auftragnehmer vereinbaren Umfang und Zeitplan dieser Maßnahmenbehandlung einvernehmlich. Die Unterrichtung des Auftraggebers zum Bearbeitungsstand der Maßnahmen erfolgt im Rahmen des Regelreportings.

Der Auftraggeber behält sich das Recht vor, den Fortschritt und Wirksamkeit der Verbesserungsmaßnahmen vor Ort durch ein anlassbezogenes Audit zu prüfen. Für die Vorbereitung dieser Prüfungen gilt der oben für Audits genannte Zeitrahmen.

d) Kalkulatorische Aufwände und Kosten

Der Auftraggeber führt anlasslose Audits abhängig von der Kritikalität der erbrachten Leistung, maximal alle zwei Jahre sowie auf standardisierter Basis und mehrheitlich als Remote-Prüfung durch. Hierbei liegt der durchschnittliche Aufwand auftragnehmerseitig für Vorbereitung und Durchführung bei ca. zwei Tagen. Für Vor-Ort-Prüfungen veranschlagt der Auftraggeber durchschnittlich fünf Tage auf Seiten des Auftragnehmers. Nicht enthalten hierin sind die Aufwände zur Bereitstellung der zu prüfenden Dokumentation. Aufwände für anlassbezogene Audits können nicht pauschal benannt werden.

Audits im Kontext kritischer Anlagen finden standardmäßig als Vor-Ort-Audit statt. Erfolgt die Leistungserbringung nicht allein durch den Auftragnehmer, kann sich das Audit auf die gesamte Lieferkette erstrecken. Der Auftragnehmer hat in seinen Verträgen die entsprechenden Voraussetzungen zu schaffen. Die Aufwände für diese Audits können höher sein, da die Inhalte durch gesetzliche und behördliche Vorgaben bestimmt werden.

Die Vertragsparteien tragen jeweils ihre im Rahmen der Audits anfallenden Kosten.