Ergänzende Vertragsbedingungen

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

– Ausgabe 01.11.2024 –

1. Allgemeines

1.1 Der Auftragnehmer liefert dem Auftraggeber durch Informationstechnologie unterstützte Dienstleistungen bzw. IT (Information Technology)- oder OT (Operational Technology)-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 Die vom Vertrag abgedeckten Informationen und Anwendungen unterliegen einem definierten Schutzbedarf (normal, hoch, sehr hoch) und gegebenenfalls speziellen gesetzlichen Anforderungen (z.B. der Gesetzgebung zu Kritischen Infrastrukturen), aus denen sich die konkrete Ausgestaltung der Maßnahmen zur Informationssicherheit ableitet. Der Schutzbedarf selbst, sowie Details zu Maßnahmen, sind in der Leistungsbeschreibung beschrieben.

1.4 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.

1.5 Soweit nicht ausdrücklich etwas anderes vereinbart wird, sind etwaige dem Auftragnehmer durch die Umsetzung der nachfolgenden Anforderungen entstehenden Aufwände mit der vereinbarten Vergütung abgegolten.

1.6 Verstößt der Auftragnehmer gegen die Verpflichtungen aus den Ziffern 2.2.a), 2.5, 2.9 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 Gewährleistung der Informationssicherheit im Rahmen der Leistungserbringung etabliert und hält dieses während der gesamten Vertragslaufzeit aufrecht. Beispielsweise geschieht dies in Form eines angemessenen Informationssicherheitsmanagementsystems (ISMS) oder durch gleichwertige, geeignete Prozesse zur Gewährleistung der Informationssicherheit im Rahmen der Leistungserbringung. Die Informationssicherheitsprozesse des Auftragnehmers entsprechen mindestens den nachfolgend beschriebenen Informationssicherheitsanforderungen und orientieren sich an der DIN EN ISO/IEC 27001/27002 oder einem gleichwertigen Rahmenwerk in der jeweils aktuellen Fassung.

2.2 Rollen und Ansprechpartner

a) Koordinator Informationssicherheit

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

b) Ansprechpartner Regelkommunikation

Der Auftraggeber kann vom Auftragnehmer verlangen, weitere Ansprechpartner / Rollenverantwortliche in allen informationssicherheitsrelevanten Angelegenheiten im Kontext der beauftragten Leistung zu benennen (z.B. fachlich, technisch oder betrieblich Verantwortliche) und die Aufgabenverteilung und den Verantwortungsübergang zweifelsfrei zu klären. Änderungen teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.

c) Ansprechpartner Notfallkoordination

Der Auftragnehmer benennt einen zentralen Ansprechpartner (SPOC / Single Point of Contact) zur Notfallkommunikation, der dem Auftraggeber zu den im Vertrag geregelten Fristen zur Verfügung steht. Der SPOC hat im Notfall Zugriff auf alle notwendigen Daten des Auftragnehmers (z.B. Produkt Monitoring, Identity Access Management (IAM) und Konfigurationsdaten) und stellt diese dem Auftraggeber und dessen Notfallteam auf Anforderung und in geeignetem Format (les- und verarbeitbar) zur Verfügung.

2.3 Sicherheitsüberprüfung

Der Auftraggeber behält sich vor, vom Auftragnehmer für Mitarbeiter oder sonstige von ihm im Rahmen der Leistungserbringung eingesetzten Personen (auch von Nachunternehmern), die im Bereich kritischer Infrastrukturen mit besonders schützenswert kategorisierten Informationen und Anlagen im Sinne der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritis-Verordnung) in Kontakt kommen, die Durchführung einer Sicherheitsüberprüfung gemäß Vorgaben des BSI in „Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen“ zu verlangen. Der Auftragnehmer bestätigt dem Auftraggeber die erfolgreiche Durchführung der Sicherheitsüberprüfung in Textform.

2.4 Statusbericht

Der Auftragnehmer liefert dem Auftraggeber auf Anforderung einen Statusbericht zur Informationssicherheit der bezogenen Leistung. Dieser enthält z.B. Informationen zu Abweichungen von vereinbarten Informationssicherheitsanforderungen und korrelierten Maßnahmen zur Behebung, Verlaufsstatistiken zu Informationssicherheitsvorfällen und Sicherheitspatches, Status Schwachstellenmanagement und Auditergebnisse, Verfügbarkeit von Security Controls, Aufwände zur Behebung von Incidents und Fakturierung bei gesonderter Vereinbarung von Sicherheitsmaßnahmen. Form, Inhalt und Frequenz werden innerhalb von acht Wochen nach Vertragsabschluss und in jedem Fall vor Betriebsbeginn bzw. der Lieferung des Produktes verpflichtend und einvernehmlich und in Textform zwischen Auftraggeber und Auftragnehmer vereinbart und orientieren sich hierbei an den Regelungsinhalten der DIN EN ISO/IEC 27001.
Ein Berichtsmuster kann auf Anfrage zur Verfügung gestellt werden.

2.5 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 weist dies dem Auftraggeber auf Anfrage nach.

2.6 Verpflichtung Nachunternehmer

Der Auftragnehmer gewährleistet, dass seine in Bezug auf dieses Vertragsverhältnis eingesetzte Nachunternehmer und deren Nachunternehmer die Anforderungen aus diesem Vertrag, die der ISO27001 oder solche einer vergleichbaren Norm erfüllen. Er stellt entsprechende Nachweise auf Anforderung des Auftraggebers zur Verfügung.

2.7 Datenverarbeitung

Verarbeitet oder speichert der Auftragnehmer Daten des Auftraggebers und der mit diesem gemäß §§ 15 ff. AktG verbundenen Unternehmen („verbundene Unternehmen“), so verpflichtet sich der Auftragnehmer sowohl regulatorische und gesetzliche Anforderungen (bezogen auf den Rechtsraum des Auftraggebers) als auch Anforderungen der Leistungsbeschreibung zu beachten und einzuhalten, insbesondere die Regelungen zur Datensicherung.

2.8 **Verschlüsselung**

Der Auftragnehmer gewährleistet eine verschlüsselte Übertragung und Speicherung von Daten der Klassifizierung "DB Vertraulich" und "DB Streng vertraulich", gemäß dem Stand der Technik. Werden kryptographische Maßnahmen während der Vertragslaufzeit unsicher, sind diese nach Absprache zu ersetzen. Die Kostenübernahme hierzu wird einvernehmlich zwischen Auftraggeber und Auftragnehmer geregelt.

2.9 **Rechtsräume Hosting / Speicherung**

Der Auftragnehmer verpflichtet sich, alle Länder, in denen Daten des Auftraggebers gehostet, gespeichert bzw. Anwendungen betrieben werden, zu benennen sowie bestehende Anforderungen aus der Leistungsbeschreibung zu bestätigen (z.B. im Rahmen des Angebots). Erfolgt die Speicherung nicht in den Systemen des Auftragnehmers, ist dies dem Auftraggeber separat anzuzeigen.
Der Auftragnehmer sichert zu, dass die Daten die benannten Speicherorte nicht verlassen. Umzüge innerhalb der EU sind hiervon ausgenommen, müssen dem Auftraggeber aber unverzüglich in Textform mitgeteilt werden.

2.10 **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.

2.11 **Endgeräte**

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 Asset des Auftragnehmers verstanden, dass an IT-/OT-Applikationen sowie IT-/OT-Infrastruktur des Auftraggebers (kabelgebunden oder kabellos) angeschlossen oder zur Verarbeitung von Daten des Auftraggebers eingesetzt wird.

- Nur vom Auftragnehmer aktiv verwaltete Endgeräte dürfen verwendet werden.
- Der Einsatz von Multi-Faktor-Authentifizierung ist anzustreben, solange nicht verbindlich in der Leistungsbeschreibung gefordert.
- Die Endgeräte müssen nach dem Stand der Technik abgesichert sein. Auf Anfrage weist der Auftragnehmer die Sicherheitsmaßnahmen nach und aktualisiert diese bei Bedarf.
- 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 Einsatz von Hacking-Tools, Sniffern, 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.

Fachlich bedingte Abweichungen sind in Textform mit dem Auftraggeber abzustimmen.

2.12 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 haben. Die Meldung hat, sofern der Informationssicherheitsvorfall relevant für die Daten und Systeme des Auftraggebers und der mit diesem verbundenen Unternehmen ist, unverzüglich zu erfolgen.

Die Meldung muss mindestens folgende Inhalte haben:

- Zeitpunkte des Vorfalls und der Vorfallserkennung,
- Betroffene Komponenten,
- Ergriffene Maßnahmen,
- Ersteinschätzung der Schwere / Kritikalität / rechtlicher Relevanz.

Vertragsspezifische Inhalte der Meldung werden innerhalb von acht Wochen nach Vertragsabschluss einvernehmlich in Textform vereinbart.

Die Meldungen erfolgen an die im Vertrag vereinbarten Kontakte, hilfsweise an folgende E-Mail-Adressen:

- DB InfraGO Fahrweg: soc-dbn@deutschebahn.com
- DB InfraGO Personenbahnhöfe: infosec.db.personenbahnhoefe@deutschebahn.com
- DB Energie: DB.Energie.SOC@deutschebahn.com
- DB AG, übrige Konzernunternehmen: security-issues@deutschebahn.com

Informationssicherheitsvorfälle, die nicht die Daten und Systeme des Auftraggebers und seiner verbundenen Unternehmen berühren, können dem Auftraggeber im Rahmen des regelmäßigen Statusberichts freiwillig offengelegt werden.

2.13 Wiederherstellung sicherer Zustand

Im Falle eines für den Auftraggeber und der mit diesem verbundenen Unternehmen relevanten Informationssicherheitsvorfalls hat der Auftragnehmer neben der Information des Auftraggebers auch 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 mit dem Auftraggeber verbundener Unternehmen und / oder Dritter notwendig, gewährt der Auftragnehmer diesen Zugang zu allen notwendigen Informationen, Systemen und Betriebsstätten.

2.14 Zugriffe

Ein direkter oder verdeckter Zugang zu den Informationssystemen (operative Systeme, Netze, Programme, Datenbestände) des Auftraggebers und der mit diesem verbundenen Unternehmen ist dem Auftragnehmer nur dann gestattet, wenn er vom Auftraggeber eine ausdrückliche, dokumentierte Zugriffsberechtigung erhalten hat; die Zugriffsberechtigung ist auf die eingesetzten und ausdrücklich zugelassenen Mitarbeiter des Auftragnehmers bzw. seiner Nachunternehmer beschränkt. Die Weitergabe der Zugriffsberechtigung an Dritte ist untersagt. Eine erteilte Zugriffsberechtigung darf ausschließlich im Rahmen der vertraglich übernommenen Leistungen genutzt werden.

2.15 Betriebssicherheit

Der Auftraggeber behält sich das Recht vor, Netzzugänge des Auftragnehmers zur Infrastruktur des Auftraggebers und seiner verbundenen Unternehmen auf Grund behördlicher Anordnungen oder mit dem Auftraggeber vereinbarter Nutzungsbestimmungen zu überwachen oder zu sperren. Ebenfalls ist eine Unterbrechung dieser Zugänge jederzeit möglich, wenn durch die an das Netz angeschlossenen Geräte des Auftragnehmers in irgendeiner Weise die Betriebssicherheit bzw. das Betriebsverhalten des Netzes oder daran angeschlossener anderer Geräte oder Software beeinträchtigt werden. Vorgenanntes gilt vorbehaltlich abweichender Regelungen zum Umgang mit personenbezogenen Daten im Auftragsverhältnis.

3. Bewertung des Reifegrads der Informationssicherheit beim Auftragnehmer

3.1 Bewertung der Sicherheitsorganisation

Der Auftragnehmer hat dem Auftraggeber auf Anforderung Informationen seiner Sicherheitsorganisation offenzulegen und auf Nachfrage geeignete Evidenzen auszuhändigen, auf deren Basis der Auftraggeber eine Bewertung des Reifegrads der Informationssicherheit durchführen kann. Dies können z.B. eine Management Summary zur Sicherheitsorganisation im Anwendungsbereich der Leistung, Berichte aus einem bestehenden Informationssicherheitsmanagementsystem, ein DIN EN ISO/IEC 27001-Zertifikat, einschließlich detaillierter Beschreibung des Geltungsbereichs und der Erklärung der Anwendbarkeit (Statement of Applicability (SoA)) und des ISO/IEC 27001–Prüfberichts bzw. äquivalente Nachweise oder aktuelle Auditergebnisse im Anwendungsbereich der Leistung sein.

3.2 Audit

Der Auftragnehmer stimmt zu, dass der Auftraggeber oder ein anderer beauftragter Dritter im Auftrag des Auftraggebers den Auftragnehmer während der Laufzeit des Vertrages in Bezug auf dessen Informationssicherheit und Einhaltung datenschutzrechtlicher Bestimmungen auditieren darf. Basis der Audits in der Informationssicherheit ist die ISO27001 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.

a) Anlasslose Audits

Zwischen den anlasslosen Audits sollen grundsätzlich mindestens zwei Jahre liegen. Deren Durchführung erfolgt zu den üblichen Geschäftszeiten. Die Dauer des Vor-Ort Auditanteils ist in Abhängigkeit mit den ausgehändigten Evidenzen und wird mit mindestens zwei Arbeitstagen veranschlagt. 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 wie z.B. Managementberichte, betriebliche Unterlagen (Konfigurations- und Berechtigungsdaten, …), Berichte aus dem ISMS, etc. zur Verfügung und kommt seinen Mitwirkungspflichten, z.B. Erteilung der notwendigen Zugriffsrechte, Bereitstellen von Dokumentationen und Zugängen, im Rahmen des Audits nach. Der Auftraggeber stellt dem Auftragnehmer die Ergebnisse des Audits in Berichtsform zur Verfügung.

Der Auftragnehmer verpflichtet sich, die als kritisch gekennzeichneten Auditergebnisse in Verbesserungsprojekten anzupassen und deren Fortschritt in der Regelkommunikation zu berichten. Auftraggeber und Auftragnehmer vereinbaren Umfang und Zeitplan dieser Verbesserungsprojekte einvernehmlich. Der Auftraggeber behält sich das Recht vor, den Fortschritt der Verbesserungsmaßnahmen vor Ort zu prüfen. Für die Vorbereitung dieser Prüfungen gilt der oben für Audits genannte Zeitrahmen.

b) Anlassbezogene Audits

Anlassbezogene Audits können in Abhängigkeit von der Schwere des Anlasses bzw. der Dringlichkeit auch kurzfristiger erfolgen.

Der Auftragnehmer stimmt darüber hinaus zu, dass der Auftraggeber im Falle eines schweren Informationssicherheitsvorfalls in Bezug auf dessen Informationssicherheit und Einhaltung datenschutzrechtlicher Bestimmungen anlassbezogen auditieren darf. Diese Regelung gilt für die Laufzeit des Vertrages. Das Audit kann durch den Auftraggeber selbst oder durch einem vom ihm beauftragten Dritten erfolgen. Der anlassbezogene Auditumfang umschließt die Umsetzung des aktuellen Stands der Technik durch den Auftragnehmer. Bei Prüfung durch einen externen Dritten, stehen dem Auftraggeber sämtliche Prüfungsergebnisse bezogen auf die vertraglich vereinbarte Dienst-/ Serviceleistung zu.

Ergibt ein anlassbezogenes Audit Erkenntnisse zu Fällen von Nicht-Einhaltung vertraglich vereinbarte Informationssicherheitsanforderungen, sowie Datenschutzbestimmungen seitens des Auftragnehmers, werden diese zeitnah in den entsprechenden Verbesserungsprojekten des Auftragnehmers behandelt, um die künftige Einhaltung sicherzustellen.

Der Auftraggeber behält sich das Recht vor, den Fortschritt der Verbesserungsmaßnahmen vor Ort zu prüfen.

c) Kalkulatorische Aufwände und Kosten

Der Auftraggeber führt Informationssicherheitsaudits in der Regel 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 ISMS-Dokumentation.

Aufwände für nicht standardisierte Audits (z.B. anlassbezogene Audits) können nicht pauschal benannt werden.

Die beim Auftraggeber anfallenden Kosten eines anlasslosen Audits werden vom Auftraggeber getragen. Die beim Auftraggeber anfallenden Kosten eines anlassbezogenen Audits werden vom Auftragnehmer getragen.

K Leistungen im Kontext wichtiger und besonders wichtiger Einrichtungen / kritischer Infrastrukturen

Die nachfolgend formulierten Anforderungen gelten für Verträge, aus denen Abrufe für die im Folgenden genannten Konzerngesellschaften erfolgen können oder die mit diesen direkt abgeschlossen sind:

Wichtige und besonders wichtige Einrichtungen

- Deutsche Bahn AG
- DB Bahnbau Gruppe GmbH
- DB Dialog GmbH
- DB Fahrwegdienste GmbH
- DB Fahrzeuginstandhaltung GmbH
- DB Kommunikationstechnik GmbH
- DB RegioNetz Infrastruktur GmbH
- DB RegioNetz Verkehrs GmbH
- Deutsche Umschlaggesellschaft Schiene - Straße (DUSS) mbH
- MegaHub Lehrte Betreibergesellschaft mbH
- Mitteldeutsche Eisenbahn GmbH
- RBH Logistics GmbH
- Regionalverkehre Start Deutschland GmbH
- UBB Usedomer Bäderbahn GmbH

Betreiber kritischer Anlagen

- DB Cargo AG
- DB Energie GmbH
- DB Fernverkehr AG
- DB InfraGO AG
- DB Regio AG
- DB Systel GmbH
- DB Vertrieb GmbH
- S-Bahn Hamburg GmbH
- S-Bahn Berlin GmbH

K.1 Systeme zur Angriffserkennung

Für IT- und OT-Produkte, die sich in einer Netzwerkinfrastruktur der als kritische Infrastruktur klassifizierten Gesellschaften des DB Konzerns befinden oder Informationen dorthin einspeisen, unterstützt der Auftragnehmer den Auftraggeber bei der Integration in das System zur Angriffserkennung (SzA) des Auftraggebers. Dies umfasst die Bereitstellung von notwendigen Informationen zur Umsetzung der Bereiche Protokollierung, Detektion und Reaktion sowie zur Nachweiserbringung.

Konkrete Umsetzung und gegebenenfalls Aufgabenverteilung, falls das IT- / OT-Produkt durch den Auftragnehmer betrieben wird, sind in der Leistungsbeschreibung beschrieben bzw. werden im Rahmen des Vertragsschlusses detailliert.

K.2 **Audits**

Abweichend von Absatz 3.2.c) finden Audits im Kontext kritischer Infrastruktur 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 Audits im Bereich Kritischer Infrastruktur können höher sein, weil die Inhalte durch gesetzliche und behördliche Vorgaben bestimmt werden. Die in 3.2.c) genannte Kostenregelung bleibt hiervon unberührt.

K.3 **Meldung und Bearbeitung von Sicherheitsvorfällen**

Ergänzend zu Absatz 2.12 hat im Falle eines erheblichen Sicherheitsvorfalls eine Erstmeldung an den Auftraggeber unverzüglich, spätestens aber 24h nach Kenntniserlangung des Sicherheitsvorfalls zu erfolgen, eine detaillierte Meldung einschließlich Auswirkungsanalyse spätestens nach 72h.

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

Im Rahmen der Behandlung des Sicherheitsvorfalls hat der Auftragnehmer entsprechende Erreichbarkeiten seines Personals zu gewährleisten.

Ein erheblicher Sicherheitsvorfall definiert sich wie folgt: Ein Sicherheitsvorfall, der entweder schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die DB-Konzernunternehmen verursacht oder verursachen kann, oder andere durch erhebliche materielle oder immaterielle Schäden beeinträchtigt oder beeinträchtigen kann.

K.4 **Unterstützung Risikomanagement**

Liefert der Auftragnehmer IT- und OT-Produkte, die sich in einer Netzwerkinfrastruktur des DB Konzerns befinden oder Informationen dorthin übertragen, unterstützt der Auftragnehmer den Auftraggeber bei der Durchführung eines angemessenen Risikomanagements. Dies beinhaltet - wo zutreffend - die Bereitstellung von Informationen zu folgenden Themenkomplexen:

- Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,
- Bewältigung von Sicherheitsvorfällen,
- Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen Auftragnehmer und von ihm beauftragter Diensteanbietern/ Lieferanten,
- Sicherheitsmaßnahmen bei Entwicklung und Wartung von IT- und OT-Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
- Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder zur kontinuierlichen Authentifizierung.

Betreibt der Auftragnehmer das IT- oder OT-System im Auftrag des Auftraggebers, stellt er dem Auftragnehmer zusätzlich Informationen zu folgenden Bereichen zur Verfügung:

- Verwendung gesicherter Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung des Auftragnehmers,
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
- grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik,
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und für das Management von Anlagen.

Der Auftragnehmer stellt diese Informationen erstmalig im Rahmen des Vertragsschlusses zur Verfügung und hält diese während der Vertragslaufzeit aktuell.

K.5 **Datensicherung / Wiederherstellung**

Der Auftragnehmer stellt dem Auftraggeber ein Konzept zur Datensicherung und Wiederherstellung (auch im Krisenfall) des IT-/OT-Systems zur Verfügung. Betreibt der Auftragnehmer das System im Auftrag des Auftraggebers, verantwortet er dessen Umsetzung.

Das Konzept beinhaltet u.a.:

- Dokumentation der Datensicherungs- und Wiederherstellungsmechanismen und -vorgehen einschließlich notwendiger Konfigurationen,
- Nachweis der korrekten Funktion der Datensicherungs- und Wiederherstellungsmechanismen,
- Auftraggeberseitige Voraussetzungen zur Implementierung des Konzepts
- Umgang mit Wechselmedien und kryptographischem Material (Schlüssel, Hashwerte, ...),
- Parameter und Konfigurationen von IT-/OT-Geräten,
- Verifikation der Datensicherungs- und Wiederstellungsvorgehen,
- Zeitpläne,
- Unabhängigkeit der Datensicherung vom normalen Betrieb,
- Protokollierung der Sicherungs- und Wiederherstellungstätigkeiten.

❑