Anhang 2 der Auftragsverarbeitungsvereinbarung

Allgemeine Rahmenbedingungen Informationssicherheit Technische und organisatorische Maßnahmen (TOMs)

Enterprise Core Services

der

BARMER und der HEK

Inhaltsverzeichnis

1 Einleitung

Dieses Dokument enthält die Mindestanforderungen zur Informationssicherheit des Auftraggebers an einen Auftragnehmer im Rahmen eines Vertragsschlusses. Ausgelegt sind diese auf den Abschluss eines Vertrages zur Auftragsverarbeitung im Sinne der DSGVO. Die Anforderungen definieren allgemeine technische und organisatorische Maßnahmen (TOMs), die der Auftragnehmer erfüllen muss. Sofern die Anforderungen in einer Leistungsbeschreibung oder weiteren vertraglichen Dokumenten seitens des Auftraggebers präzisiert, erweitert oder abgegrenzt sind, gelten diese ebenfalls, wobei im Fall von Widersprüchen 1) stets das höhere Sicherheitsniveau gilt und 2) die weitreichendere Informations-Kenntnis des Auftraggebers zu wahren ist.

Die in diesem Dokument beschriebenen Anforderungen und Maßnahmen wurden gewählt, um die Schutzziele der Informationssicherheit (Vertraulichkeit, Verfügbarkeit, Integrität) und des Datenschutzes[1] im Rahmen einer Auftragsverarbeitung angemessen zu gewährleisten, insbesondere zur Wahrung der Rechte Betroffener.

Die technische Umsetzung ist vom Auftragnehmer nach dem **Stand der Technik** zu gestalten und laufend sowie unaufgefordert neuen Entwicklungen anzupassen. Als Maßgabe und Referenz wird das jeweils aktuelle Dokument zum Stand der Technik vom TeleTrusT[2] zugrunde gelegt.

2 Dienstleistungen im KRITIS-Umfeld

Der Auftragnehmer erbringt für den Auftraggeber Dienstleistungen, die den gesetzlichen KRITIS-Regularien nach §8a BSIG unterliegen[3]. Der Auftraggeber benennt die Teile der Dienstleistung, die unter die KRITIS-Regularien fallen, allgemein in der **01-02 Leistungsbeschreibung** sowie im **01-02-01 Service Katalog** und im Detail spätestens während der Transition; diese können sich während der Vertragslaufzeit ändern (bspw. aufgrund von Gesetzesänderungen oder Änderungen beim Auftraggeber) und werden dem Auftragnehmer vom Auftraggeber bekanntgegeben. Der Auftragnehmer verpflichtet sich, eigenständig auf die Einhaltung der gesetzlichen und regulatorischen KRITIS-Rahmenbedingungen zu achten, soweit sie die erbrachte Dienstleistung und den Auftragnehmer in der Rolle des Dienstleisters betreffen. Dasselbe gilt für die im B3S GKV/PV dargelegten Rahmenbedingungen; vgl. u.a. § 392 SGB V, Absatz 6.

Bei der Durchführung von KRITIS-Audits des Auftraggebers, die die Leistungen des Auftragnehmers zum Gegenstand haben, verpflichtet sich der Auftragnehmer zur Mitarbeit bei der Vorbereitung und während des KRITIS-Audits; insbesondere sind nach Absprache qualifizierte Ansprechpersonen bereitzustellen. Dasselbe gilt für die Bereitstellung von Räumlichkeiten für eine mögliche Prüfung vor Ort und Dokumentation, die der Auftraggeber zum Nachweis der KRITIS-Kon-

[1] Gem. „Standard Datenschutzmodel (SDM)“ der Datenschutzkonferenz: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V31.pdf

[2] Das Dokument zum Stand der Technik kann auf der Seite des TeleTrusT aufgerufen werden: https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

[3] Die KRITIS-Prozesse der gesetzlichen Kranken- und Pflegeversicherung können dem aktuellen B3S GKV/PV (Branchenspezifischer Sicherheitsstandard der gesetzlichen Kranken- und Pflegeversicherer) entnommen werden: https://www.bsi.bund.de/SharedDocs/Textbausteine/DE/KRITIS/B3S/Finanz-Versicherungswesen/b3s-gkv-pv.html?nn=126610

formität vom Auftragnehmer benötigt. Dies gilt auch für alle Unterauftragnehmer des Auftragnehmers, wobei der Auftragnehmer verpflichtet ist, seine Unterauftragnehmer hinsichtlich des Audits zu steuern und zu koordinieren.

Sollten im Rahmen eines KRITIS-Audits Mängel benannt werden, die auf die Dienstleistung des Auftragnehmers (oder ggf. eingesetzter Unter-Auftragnehmer des Auftragnehmers) zurückzuführen sind, so verpflichtet sich der Auftragnehmer, diese in den gesetzlich oder von der jeweiligen Aufsichtsbehörde vorgeschriebenen Zeitfenstern zu beheben. In Fällen, in denen keine behördlichen oder gesetzlichen Fristen bestehen, hat der Auftragnehmer die Mängel innerhalb einer angemessenen, vom Auftraggeber gesetzten Frist zu beheben. Die Behebung der Mängel ist mit dem Auftraggeber abzustimmen und zu dokumentieren, der Auftragnehmer informiert den Auftraggeber regelmäßig und auf Nachfrage über den Fortschritt und den fristgerechten Vollzug erforderlicher Korrekturmaßnahmen.

3 Personelle Anforderungen

3.1 Ansprechpersonen für IT- und Informationssicherheit

Der Auftragnehmer hat gegenüber dem Auftraggeber eine fachlich qualifizierte Ansprechperson für Informationssicherheit und eine fachlich qualifizierte Ansprechperson für IT-Sicherheit zu benennen; hierbei kann es sich um dieselbe Person handeln. Zusätzlich ist jeweils eine Vertretung vorzusehen. Die Ansprechpersonen beherrschen die Sprache Deutsch in Wort und Schrift mindestens nach Sprachniveau C2 gemäß dem europäischen Referenzrahmen. Kontaktdaten der Ansprechpersonen für Informationssicherheit und IT-Sicherheit werden dem Auftraggeber spätestens 10 Tage nach Vertragsschluss und nicht später als zum Start der Transition zum Zweck der direkten Kontaktaufnahme im Anhang 5 der **02-09-02 Auftragsverarbeitungsvereinbarung** – siehe **02-09-04 AVV Anhang (3-5)** – mitgeteilt.

3.2 Regelmäßige Schulungen

Neu eingestellte Personen müssen vom Auftragnehmer eingearbeitet und eingewiesen werden. Dies beinhaltet insbesondere:

- Die Einarbeitung im Bereich der Informationssicherheit mit Information über die für die Aufgabenerfüllung relevanten Informationssicherheits-Regelungen.
- Die Information, welcher rechtliche Rahmen die Tätigkeit bestimmt und welche bestehenden Gesetze, Vorschriften und Regelungen einzuhalten sind.

Darüber hinaus sind alle Beschäftigten in regelmäßigen Abständen – mindestens jedoch einmal jährlich – im Rahmen interner Informationsveranstaltungen in den vorgenannten Themen zu schulen und zu sensibilisieren. Nachweise zu durchgeführten Schulungen sind auf Nachfrage dem Auftraggeber vorzulegen.

3.3 Überprüfung bei administrativen Tätigkeiten

Bei administrativen Tätigkeiten (IT- und Systemadministration) sind die damit betrauten Personen, neben den gesetzlich erforderlichen Überprüfungen, vor der Tätigkeitsaufnahme angemessen vom Auftragnehmer zu überprüfen, bspw. durch die Vorlage und Sichtung eines Führungszeugnisses. Falls Bedenken bestehen, ist die Person von der Tätigkeit für den Auftraggeber auszuschließen.

4 Anforderungen an das Informationssicherheits-Managementsystem (ISMS)

Der Auftragnehmer hat seine Dienste und Leistungen nach den Maßgaben des jeweils geltenden ISO/IEC Standards 27001 für ein ISMS zu betreiben. Dies gilt sowohl für die IT-Systeme, die zur Erbringung der Dienstleistung erforderlich sind, als auch für die organisatorischen und personellen Rahmenbedingungen.

Eine gültige Zertifizierung nach der jeweils geltenden ISO/IEC 27001, ggf. ISO/IEC 27001 nach BSI IT-Grundschutz, ist über die gesamte Vertragslaufzeit und ohne Unterbrechung aufrecht zu erhalten. Dabei muss der Geltungsbereich die gesamte, in der Leistungsbeschreibung und weiteren vertraglichen Dokumenten geforderte Dienstleistung umfassen (Eignungsleihe und Unterauftragsvergabe, siehe Abschnitt 4.1). Der Auftragnehmer hat den Auftraggeber zeitnah (spätestens 10 Kalendertage nach Vorliegen des Audit-Ergebnisses) und unaufgefordert über das Ergebnis einer Re-Zertifizierung zu informieren und – soweit erteilt – das neue Zertifikat digital vorzulegen.

Der Auftraggeber hat jederzeit das Recht, das Zertifikat des Auftragnehmers digital einzusehen. Dasselbe gilt für das zugehörige SoA („Statement of Applicability“ bzw. „Erklärung zur Anwendbarkeit“) unter Wahrung der Geschäftsgeheimnisse des Auftragnehmers.

4.1 Unterauftragsvergabe und Eignungsleihe ISO/IEC 27001

Kann der Auftragnehmer die gesamte von ihm geforderte Leistung nicht über eine eigene Zertifizierung nach ISO/IEC 27001 abdecken und bedient sich daher Unter-Auftragnehmern, die ein entsprechendes Zertifikat nach ISO/IEC 27001 vorweisen können, so gilt folgendes: Der Auftragnehmer muss sicherstellen, dass die gesamte erbrachte Leistung über eine oder mehrere ISO/IEC 27001-Zertifizierungen abgedeckt ist. Der Auftragnehmer ist für die Steuerung und Kontrolle seiner Unter-Auftragnehmer verantwortlich und muss den Auftraggeber jederzeit über den aktuellen Stand der Zertifizierungen seiner Unter-Auftragnehmer informieren können. Darüber hinaus muss der Auftragnehmer die Steuerung der Unter-Auftragnehmer (Providermanagement), bei denen die Eignungsleihe oder Unterauftragsvergabe Anwendung findet, in seiner eigenen Zertifizierung nach ISO/IEC 27001 abgedeckt haben und dies dem Auftraggeber darlegen[4].

Der Auftragnehmer ist verpflichtet, dem Auftraggeber schriftlich darzulegen, wie die Zertifizierung nach ISO/IEC 27001 über den Auftragnehmer und seine Unter-Auftragnehmer abgedeckt ist. Diese Information ist dem Auftraggeber bei Angebotsabgabe im Grobkonzept zur Sicherheitskonzept-Erstellung und darüber hinaus spätestens jährlich (Intervall beginnend mit Datum des Vertragsschlusses) und verpflichtend bei

a) jedem Wechsel eines Unter-Auftragnehmers,
b) bei jeder Erneuerung oder fehlgeschlagenen Re-Zertifizierung eines relevanten Zertifikats (binnen 10 Tagen nach Vorliegen des Audit-Ergebnisses bei der auditierten Stelle) und
c) auf Anfrage des Auftraggebers binnen zwei Wochen vorzulegen

und enthält mindestens die folgenden Informationen:

i. Aufstellung sämtlicher für den Auftraggeber erbrachten Leistungen sowie einen eigenen Punkt zur Koordination der Unter-Auftragnehmer,
ii. Zuordnung, welche Leistung von welchem (Unter-)Auftragnehmer erbracht wird,

[4] Die Koordination von Dienstleistern ist Teil des ISMS nach ISO/IEC 27001 und daher nicht an ein Dritt-Unternehmen übertragbar.

iii. Zuordnung des relevanten Zertifikats nach ISO/IEC 27001 des (Unter-)Auftragnehmers zu der jeweiligen Leistung inkl. Gültigkeitsdatum,
iv. Zuordnung des Geltungsbereichs und weiterer, relevanter Informationen des Zertifikats (bspw. Standorte) zur jeweiligen Leistung und Darlegung, wieweit die Zertifizierung die Leistung abdeckt,
v. sämtliche referenzierte Zertifikate nach ISO/IEC 27001 in digitaler Form.

Auf Rückfragen des Auftraggebers hat der Auftragnehmer binnen einer Woche zu antworten. Das Recht, das SoA des Auftragnehmers einzusehen (vgl. Abschnitt 4), gilt bei dann analog für die Unter-Auftragnehmer des Auftragnehmers.

5 Sicherheit der IT-Infrastruktur

Der Auftragnehmer hat alle technischen und organisatorischen Maßnahmen für einen gesicherten Betrieb, zur Notfallvorsorge (siehe auch Abschnitte 5.1 und 8) sowie zum Schutz gegen unbefugte Nutzung oder Änderung der genutzten Infrastruktur zu ergreifen und ausreichend zu dokumentieren (vgl. auch Anforderungen der DSGVO Art. 32).

Der Auftragnehmer stellt eine hinreichende, dem Stand der Technik entsprechende Überwachung seiner eigenen Systeme und Netzwerke sicher. Beispiele hierfür können Firewall-Systeme oder Intrusion Detection- / Prevention System (IDS[5], IPS[6]) sein. Der Auftragnehmer kann alternative oder zusätzliche technische und organisatorische Maßnahmen einsetzen, sofern diese ein vergleichbares Sicherheitsniveau gewährleisten und dies gegenüber dem Auftraggeber nachgewiesen wird. Ein Abfluss von Daten des Auftraggebers ist durch technische und organisatorische Maßnahmen zuverlässig zu verhindern.

5.1 IT-Service Continuity Management (IT-SCM) System

IT-Service Continuity Management (IT-SCM) stellt sicher, dass die durch den Auftragnehmer erbrachten IT-Services gemäß Leistungsbeschreibung und SLA auch im Notfall und bei größeren Schadensereignissen erbracht werden. Das IT-SCM ist in das Business Continuity Management (BCM) des Auftragnehmers integriert (siehe auch Abschnitt 8).

Der Auftragnehmer verfügt über ein integriertes IT-SCM-System. Die Wirksamkeit der getroffenen Maßnahmen ist regelmäßig vom Auftragnehmer zu überprüfen. Dies beinhaltet eine jährliche Planung, Durchführung und Dokumentation von Notfallübungen, siehe auch Abschnitt 8.3.1.

5.2 Rechenzentrum und Netzzugang

Die örtlichen Gegebenheiten des Auftragnehmers, insbesondere des Rechenzentrums, müssen geeignete Einrichtungen und Verfahren zu den folgenden Punkten haben: Zugangskontrollsystem, Raumklimatisierung, Blitzschutzeinrichtung, Stromversorgung (bei Rechenzentren redundant), Gefahrenmeldeanlage und Brandschutz.

Für ein Rechenzentrum, das zur Leistungserbringung eingesetzt wird, muss die Erfüllung an Standortsicherheit und Rechenzentrumsbetrieb gemäß Tier-3[7] nachgewiesen werden.

[5] Intrusion Detection Systeme

[6] Intrusion Prevention Systeme

[7] Tier-3 gemäß dem etablierten Standard des Uptime Institute

Die Sicherheit des Netzzugangs ist mittels Vorlage eines erfolgreichen Penetrationstests (nicht älter als 1,5 Jahre und ggf. vor Erstinbetriebnahme) nachzuweisen. Die Person, die den Penetrationstest durchführt, muss entsprechend qualifiziert sein, bspw. durch eine Zertifizierung vom BSI bzw. mindestens 3-jähriger einschlägiger Praxiserfahrung.

5.3 System-Wartung, System-Pflege und System-Härtung

Alle Maßnahmen zur Aufrechthaltung eines sicheren und ordnungsgemäßen Systembetriebes, wie z. B. Software- und Hardware-Updates/Upgrades, sind ein Bestandteil der durch den Auftragnehmer zu erbringenden Leistung. Der Auftragnehmer hat dafür Sorge zu tragen, dass Hardware, Betriebssysteme und Anwendungen durch Aktualisierungen auf einem sicheren und stabilen Stand gehalten werden. Dazu muss ein geordneter Prozess beim Auftragnehmer dokumentiert und etabliert sein.

Der Auftragnehmer härtet alle seine und – soweit es in seinem Zuständigkeitsbereich liegt – die für den Auftraggeber betriebenen Anwendungen, IT-Systeme und Schnittstellen regelmäßig nach aktuellen, anerkannten Standards wie bspw. den CIS Controls oder NIST SP 800-53.

Sicherheits-Updates und -Patches sind schnellstmöglich (d.h., bei kritischer bis hoher Gefährdung nach CVSS-Klassifizierung binnen weniger Tage) nach Bekanntgabe durch die Hersteller und ggf. erforderlichen Kompatibilitätstests zu installieren. Aus den Aktualisierungen darf grundsätzlich keine nachhaltige Betriebsstörung oder -gefährdung resultieren. Entsteht bspw. aus Betriebsgründen dennoch ein höheres Sicherheitsrisiko für die Daten des Auftraggebers, **so ist der Auftraggeber unverzüglich zu informieren** und weitere Schritte mit dem Auftraggeber abzustimmen, wobei der Auftragnehmer im Zweifelsfall eigenständig an einer zeitnahen Risiko-Reduktion arbeitet. Es ist dabei unerheblich ob bekannt ist, ob die Schwachstelle(n) bereits ausgenutzt werden.

Die Release-Stände eingesetzter Software und Betriebssysteme sind in geeigneter Weise zu dokumentieren und – soweit vertraglich vereinbart – über technische Schnittstellen an den Auftraggeber zu übermitteln (siehe auch **02-02 Technologiegrundsätze**). Spätestens auf Anfrage gewährt der Auftragnehmer dem Auftraggeber anlassbezogen Einsicht in die Patch-Stände der für den Auftraggeber betriebenen Systeme.

5.4 Schutz vor Schadsoftware

Es muss eine Software zur Erkennung von und dem Schutz vor Schadsoftware eingesetzt werden, die routinemäßig Computer und Medien scannt. Diese muss in aktueller Version eingesetzt werden und in der Lage sein, tagesaktuelle Bedrohungen zu erkennen. Die Art und Implementierung der Erkennungssoftware muss nach den aktuellen Empfehlungen des Herstellers verwendet werden.

Es müssen Verfahren und Verantwortlichkeiten zum Umgang mit dem Schadsoftware-Schutz auf den Systemen, zur Nutzungsschulung, zur Meldung über Schadsoftware-Angriffe (siehe auch Abschnitt 9 für Meldungen an den Auftraggeber) und zu zeitnahen Wiederherstellungsmaßnahmen (siehe auch Abschnitt 8) festgelegt werden.

5.5 Sonderregelungen bei Cloud-Dienstleistungen

Kommt zur Erfüllung der vereinbarten Leistung ein Cloud-Computing-Dienst zum Einsatz oder ist selbst Leistungsgegenstand, so gelten die Anforderungen aus § 393 SGB V[8] für die gesamte Zeit der Leistungserbringung. Das nach § 393 SGB V geforderte C5-Testat[9] muss dem Auftraggeber vor Beginn der Datenverarbeitung vom Auftragnehmer vorgelegt werden und bei einer Re-Testierung während der Vertragslaufzeit unaufgefordert binnen 2 Wochen nach Ausstellung des neuen Testats. Dies gilt auch, falls der Auftragnehmer nicht selbst Cloud-Dienstleister ist, sondern zur Leistungserbringung auf die Dienste eines Cloud-Anbieters zurückgreift.

Die Daten des Auftraggebers sind auch in der Cloud verschlüsselt abzulegen (vgl. Abschnitt 7.2). Dabei liegt die Schlüsselhoheit beim Auftraggeber (BYOK – Bring Your Own Key) und nicht beim Auftragnehmer bzw. Cloud-Betreiber.

6 Regelungen für Zutritt, Zugang, Zugriff

6.1 Zutritt

Der Auftragnehmer muss Sorge tragen, dass nur autorisiertes Personal Zutritt zu den Räumlichkeiten hat, in denen Daten des Auftraggebers verarbeitet werden. Diese Zutritte sind angemessen zu dokumentieren.

6.2 Zugang

Der Auftragnehmer muss sicherstellen, dass nur das für die Leistungserbringung autorisierte Personal Zugang zu den Systemen hat, mit denen Daten des Auftraggebers verarbeitet werden. Diese Zugänge sind angemessen zu dokumentieren.

6.3 Zugriff

6.3.1 Authentifizierung und Autorisierung

Ohne Authentifizierung und Autorisierung darf kein Zugriff auf die zur Leistungserbringung eingesetzten Systeme erfolgen. Deshalb sind durch den Auftragnehmer angemessene Authentifizierungsmechanismen nach Stand der Technik zu implementieren.

Der Auftragnehmer hat für die im Rahmen der Leistungserbringung genutzten IT-Systeme und Anwendungen geregelte Verfahren zu Vergabe, Änderung, Entzug und Prüfung von Benutzerrechten für alle intern und extern Beschäftigten umzusetzen. Es gilt das Prinzip des „least-privilege“, das als Konzept besagt, dass einem Beschäftigten nur die Rechte vergeben werden, die

[8] Sollte sich der gesetzliche Rahmen zu § 393 SGB V während der Vertragslaufzeit ändern, so gelten im Zweifelsfall die Anforderungen, die nach Dafürhalten des Auftraggebers ein höheres Sicherheitsniveau darstellen, mindestens aber die gesetzlichen Anforderungen.

[9] Zur Vorlage eines vergleichbaren Nachweises, siehe die C5-Gleichwertigkeitsverordnung vom 19.03.2025. Hinweis: Je nach Aufteilung der Dienste und Services kann die Vorlage mehrerer C5-Testate durch den Auftragnehmer erforderlich sein.

er zur Erfüllung seiner Aufgaben benötigt, und diese Rechte werden zeitnah wieder entzogen, wenn sich der Aufgabenbereich ändert.

6.3.2 Zugriffsprotokollierung für Systeme

Der Zugriff auf die im Rahmen der vereinbarten Leistung eingesetzten Systeme und dort gespeicherten Daten muss für Revisionszwecke nachvollziehbar sein. Durch den Auftragnehmer ist daher für jedes System, das für die Leistungserbringung eingesetzt wird10, eine angemessene Protokollierung sämtlicher Zugriffe einzurichten. Dies gilt in besonderem Maße, aber nicht ausschließlich, wenn ein System aus dem Internet erreichbar ist.

6.3.3 Administrative Zugriffe

Administrative Zugriffe auf die für die Leistungserbringung betriebenen Systeme sind zu protokollieren, so dass bei Verdachtsfällen oder IT-forensischen Untersuchungen Zugriffe auf Systeme und Daten durch einzelne Personen einwandfrei und unzweifelhaft nachvollzogen werden können. Kritische Zugriffe, wie z.B. erfolgte Änderungen an Sicherheitseinstellungen oder nicht-autorisierte Datenbankzugriffe, sind zu analysieren. Die Protokolldateien sind gemäß den geltenden gesetzlichen Vorgaben aufzubewahren.

Grundsätzlich sind operative und administrative Zugriffe zu trennen. D.h., durch einen administrativen Zugriff darf kein Zugriff auf die verarbeiteten Daten erfolgen. Ausnahmen sind entsprechend zu dokumentieren, sachlich zu begründen und dem Auftraggeber vorzulegen.

Administrative Accounts sind durch eine Mehr-Faktor-Authentifizierung abzusichern, wobei mindestens zwei Faktoren zum Einsatz kommen müssen. Administrative Zugriffe sind zeitlich zu begrenzen, bspw. durch ein systemseitiges automatisiertes Ausloggen.

6.3.4 Protokollierung des Zugriffs auf personenbezogene Daten und Sozialdaten

Analog zur Protokollierung von administrativen Zugriffen hat der Auftraggeber bei personenbezogenen Daten und Sozialdaten eine besondere Sorgfaltspflicht. Daher müssen die Protokolldateien des Auftragnehmers Auskunft darüber geben können, wer, wann, welche Daten in welcher Weise verarbeitet hat, ggf. auch im Rahmen einer IT-forensischen Untersuchung bei einem Sicherheitsvorfall. Die Tätigkeiten der

- Authentifizierung und Autorisierung,
- Dateneingabe und -veränderung,
- Dateneinsicht,
- Datenübermittlung und
- Datenlöschung

müssen protokolliert werden.

Die Protokolldateien sind gemäß den geltenden gesetzlichen Vorgaben aufzubewahren.

[10] Für die Protokollierung auf Systemen des Auftraggebers, die abhängig vom Auftragsgegenstand vom Auftragnehmer mitgenutzt werden, ist der Auftraggeber verantwortlich und nicht der Auftragnehmer.

7 Sicherheit der Daten

7.1 Mandantenfähigkeit

Grundsätzlich können mandantenfähige Systeme für die in der Leistungsbeschreibung geforderten Dienste eingesetzt werden, sofern dies nicht vertraglich anders geregelt wurde. Soweit für den Auftraggeber besonders kritische Daten verarbeitet werden (Sozialdaten, Personaldaten oder unternehmenskritische Daten), ist ein System einzusetzen, das eine strikte Trennung von Mandanten und das Löschen der Daten gemäß Abschnitt 7.4 ermöglicht.

Es ist sicherzustellen, dass Daten des Auftraggebers nie in den Besitz Dritter gelangen oder von Dritten eingesehen werden können.

7.2 Verschlüsselte Ablage von Sozialdaten und personenbezogenen Daten

Der Auftraggeber gibt die Verschlüsselung der verarbeiteten Daten – insbesondere der Sozialdaten und personenbezogenen Daten – bei Ablage (Speicherung) der Daten an den Auftragnehmer vor. Änderungen bei der Verschlüsselung werden über einen Change Request beauftragt und sind Bestandteil der zu erbringenden Leistung. Als Referenz gelten die technischen Richtlinien des BSI (vgl. auch §95 SGB IV) wie bspw. BSI TR-02102.

Der Auftraggeber kann auf Anweisung die Umstellung der Verschlüsselungsverfahren auf quantensichere Verfahren verlangen, sofern diese verfügbar und technisch sowie wirtschaftlich umsetzbar sind, selbst wenn diese noch nicht dem Stand der Technik entsprechen. Der Auftragnehmer hat dies binnen eines halben Jahres in Abstimmung mit dem Auftraggeber umzusetzen. Falls eine Umstellung nicht oder nicht innerhalb des vorgegebenen Zeitraums möglich ist, so hat der Auftragnehmer dies sachlich begründet darzulegen und in Abstimmung mit dem Auftraggeber risikobasierte Mitigationsmechanismen auszuarbeiten und umzusetzen.

Die eingesetzten Verschlüsselungsverfahren und -protokolle sind zu dokumentieren, bspw. in einem Verfahrens- oder Betriebshandbuch.

7.3 Sicherer Transport von Daten

Der Auftragnehmer muss sicherstellen, dass jegliche Übertragung von Daten im Leistungsumfang unabhängig vom Medium durch eine angemessene Verschlüsselung geschützt wird, soweit die Übertragung und somit die Verschlüsselung im Zuständigkeitsbereich des Auftragnehmers liegen. Es gelten dieselben Hinweise und Anforderungen, insbesondere zu quantensicheren Verfahren, wie in Abschnitt 7.2. Die eingesetzten Verschlüsselungsverfahren und -protokolle sind zu dokumentieren, bspw. in einem Verfahrens- oder Betriebshandbuch.

Für den E-Mail-Verkehr zwischen Auftragnehmer und Auftraggeber muss mindestens eine Transport-Verschlüsselung durch Enforced Transport Layer Security (Enforced TLS) zum Einsatz kommen. Die Version wird durch den Auftraggeber vorgegeben. Der unverschlüsselte Versand von E-Mails im fachlichen Rahmen dieser Leistungserbringung ist auszuschließen.

Sollen per E-Mail personenbezogene Daten übertragen werden, welche besonders schützenswert sind oder bei einem Vertraulichkeitsbruch voraussichtlich ein hohes Risiko für die betroffene Person darstellen, so muss die Übertragung per E-Mail zusätzlich durch S/MIME abgesichert sein.

7.4 Löschen von Daten

Es gelten die in **02-09-02 Auftragsverarbeitungsvereinbarung** festgelegten Regelungen zum Löschen und zur Rückgabe von vertragsgegenständlichen Daten.

Wenn personenbezogene Daten temporär zum Zweck des Daten-Austauschs auf Datenspeichern abgelegt werden (bspw. Festplatte, Daten-Austauschplattform, E-Mail), so müssen diese unmittelbar, spätestens aber 72 Stunden nach der Übermittlung, vollständig von dem Speichermedium gelöscht werden.

7.5 Backup und Recovery

Alle für den Betrieb der vertraglich vereinbarten Leistung bereitgestellten Daten des Auftraggebers sind ordnungsgemäß zu sichern (Backup). Die ordnungsgemäße Sicherung umfasst mindestens die folgenden Punkte:

- Termingerechte Durchführung aller vorgesehenen Sicherungsläufe gemäß Backup-Plan.
- Inhaltliche Vollständigkeit der Datensicherungen.
- Prüfung und Kontrolle der Sicherung anhand der Sicherungsprotokolle und mit Hilfe von regelmäßigen Wiederherstellungstests.
- Erneute Datensicherung im Fehlerfall, bis eine einwandfreie Sicherung vorliegt.
- Die datenschutzgerechte Verwaltung der Sicherungsmedien erfolgt in Übereinstimmung mit der Backup- und Archivierungsstrategie. Die konkreten Verfahren, welche Daten wie und wie lange archiviert oder aufbewahrt werden müssen und ab wann eine Löschung zu erfolgen hat, sind im Einzelfall festzulegen.
- Datenwiederherstellung (Recovery), die im Bedarfsfall die Einhaltung der vertraglich geforderten Service-Level-Anforderungen/Verfügbarkeiten ermöglicht.
- Das Backup erfolgt verschlüsselt, wobei sich das Mindest-Sicherheitsniveau vom Schutzniveau der Daten ableitet.
- Backup-Medien müssen bei Außerbetriebnahme gemäß den Bestimmungen aus **02-09-02 Auftragsverarbeitungsvereinbarung** sicher gelöscht und entsorgt werden.

Der Verlauf der Datensicherungen ist kontinuierlich zu überwachen und zu protokollieren.

8 Business Continuity Management (BCM)

Für den zu erbringenden Leistungsbereich sind beim Auftragnehmer Vorkehrungen für Notfälle und Krisen zu treffen (Business Continuity Management, BCM). Der Prozess orientiert sich dabei an der ISO 22301 oder vergleichbaren einschlägigen Normen und Vorgaben. Der Auftragnehmer arbeitet im Not- und Krisenfall konstruktiv mit dem Auftraggeber zusammen, um eine schnelle Rückkehr in den Normalbetrieb zu ermöglichen.

8.1 Notfall- und Krisenorganisation

Eine Notfall- und Krisenorganisation zur zielgerichteten und raschen Bewältigung eines BCM-Ereignisses muss beim Auftragnehmer definiert und etabliert sein. Die dazu notwendigen Aufgaben, Zuständigkeiten sowie die erforderlichen Fähigkeiten und Kenntnisse müssen beim Auftragnehmer vorhanden sein. Die festgelegten Rollen müssen durch qualifizierte Mitarbeiter besetzt sein, diese müssen regelmäßig und bedarfsgerecht geschult werden.

8.2 Strategien bzw. Konzepte und Ablaufpläne

Es müssen Business Continuity (BC)-Strategien definiert sein, die verschiedene relevante Ausfallszenarien abdecken (z. B. Gebäudeausfall, IT-Ausfall wie bspw. Serverausfälle oder Netzwerkprobleme, Personalausfall, Ausfall von Externen/relevanten Dritten). Zeitkritische Geschäfts-

prozesse und Ressourcen müssen regelmäßig identifiziert und analysiert werden. Für die so identifizierten Geschäftsprozesse und Ressourcen sollten regelmäßig relevante Risiken identifiziert und analysiert werden; diese müssen angemessen behandelt werden.

Es müssen Service Continuity Pläne (SCP) vorhanden sein, mit denen die für die erbrachte Dienstleistung relevanten, zeitkritischen Geschäftsprozesse zeitgerecht und entsprechend den vertraglichen Vereinbarungen fortgeführt und die entsprechenden Ressourcen wiederanlaufen und wiederhergestellt werden können.

8.3 Regelmäßige Übung und Überprüfung

Der Auftragnehmer muss regelmäßig überprüfen, ob das BCM angemessen, wirksam und effizient ist bzw. ob Korrekturbedarfe oder Verbesserungsmöglichkeiten bestehen.

Die konkreten BC-Strategien und -Lösungen sind regelmäßig zu überprüfen. Alle relevanten BC-Pläne und BC-Maßnahmen müssen angemessen geübt und getestet werden. Die Durchführung der Übungen ist zu dokumentieren.

8.3.1 Übungen im IT-SCM

Bei Tests bzw. Übungen zum IT-Service Continuity Management (IT-SCM) ist die Wirksamkeit und Angemessenheit der Notfallvorsorge sämtlicher durch den Auftragnehmer für den Auftraggeber betriebenen IT-Services jeweils im Abstand von maximal 12 Monaten durch Tests zu überprüfen.

Dafür ist eine Testjahresplanung aufzustellen. Diese wird vom Auftragnehmer in Abstimmung und Zusammenarbeit mit dem Auftraggeber spätestens im November für das darauffolgende Kalenderjahr vereinbart. Alle technischen Tests sind mit einer Vorlaufzeit von mindestens 2 Monaten über den regulären Change-Prozess anzumelden. Wiederholungen von Tests und Übungen sind explizit im Leistungsumfang enthalten (siehe auch Abschnitt 8.3.1.4).

Auftraggeber und Auftragnehmer stimmen darin überein, dass es bei der Durchführung von Tests und Übungen zu Verletzungen der vereinbarten Service Level für die getesteten IT-Services bzw. System- und/oder Serviceumgebungen kommen kann. Die Auswirkungen sind so gering wie möglich zu halten, absehbare Störungen sind im Vorfeld mit dem Auftraggeber abzustimmen.

Im Folgenden werden drei Test- bzw. Übungsarten unterschieden:

8.3.1.1 Tests, welche der Auftragnehmer intern und selbständig durchführt

Diese Tests weisen die technische Notfallfähigkeit und die Wiederherstellung sämtlicher vom Auftraggeber ausgelagerten IT-Services beim Auftragnehmer nach. Dazu zählen u.a.:

- Szenarien-basierte Tests (z.B. Ausfall Netzwerk, Ausfall gesamter Rechenzentrums-Standort)
- Notbetrieb und Wiederherstellung von (Cloud-)Systemen und Infrastruktur
- Funktionstests bei gravierenden Veränderungen im Data Center-Betrieb
- Backup und Restore-Tests:
    - je eingesetztem Sicherungsverfahren und je Datenbank ist mindestens eine Datenwiederherstellung durchzuführen
    - Eignungstests zur Wiederherstellung der Remote Backups des Auftraggebers

Der Auftraggeber ist im Vorfeld über solche Tests zu informieren.

8.3.1.2 Tests, welche gemeinsam vom Auftragnehmer und Auftraggeber durchführt werden

Diese Tests weisen die Notfallfähigkeit und Wiederherstellung gesamter Prozessketten nach, die vom Verantwortungsbereich des Auftragnehmers in den Verantwortungsbereich des Auftraggebers übergehen. Beispiele sind Systemabschaltung und Wiederherstellung (ggf. inklusive Datenbank und Datensicherung) und Rechenzentren-Schwenktests.

Den konkreten Zeitpunkt der Übung legt der Auftraggeber in Abstimmung mit dem Auftragnehmer fest. Für jede gemeinsame Übung ist ein detailliertes Übungskonzept (inklusive Playbook) durch den Auftragnehmer zu erstellen; dieses ist mit dem Auftraggeber und ggf. weiteren Beteiligten abzustimmen. Alle an dem Test beteiligten Parteien stellen für jede Übung einen zentralen Ansprechpartner bereit. Der Haupt-Koordinator der Übung wird jeweils im Vorfeld festgelegt.

Je ausgelagertem IT-Service ist mindestens jährlich eine solche Notfallübung durchzuführen. Die jährlich einmalige Durchführung ist im Leistungsumfang enthalten, zusätzliche Notfallübungen zu einem IT-Service werden gesondert vom Auftraggeber beim Auftragnehmer beauftragt.

8.3.1.3 Organisatorische Tests

Diese Tests zielen auf die Ebene der Alarmierung, Eskalation und Zusammenwirken der Notfallorganisationen des Auftragnehmers, Auftraggebers und weiterer beteiligter Dienstleister ab.

8.3.1.4 Anforderungen an die Test-Nachbearbeitung

Die Ergebnisse der Tests und Übungen sind – bezogen auf die durch den Auftragnehmer für den Auftraggeber erbrachten Leistungen – durch den Auftragnehmer schriftlich zu dokumentieren und dem Auftraggeber spätestens vier Wochen nach der Durchführung digital zur Verfügung zu stellen.

Nicht erfolgreiche Tests sind unverzüglich durch den Auftragnehmer zu analysieren und Fehlerursachen zu beheben. Ist ein Test nicht erfolgreich, so ist dieser zu wiederholen bis der Notbetrieb und die Wiederherstellung erfolgreich nachgewiesen sind.

8.4 Ablauf im Not- und Krisenfall

Es müssen Sofortmaßnahmen definiert sein, die unmittelbar nach Eintritt eines Schadensereignisses eingeleitet werden können, um weitere Schäden abzuwenden. Regelungen zur Notfallkommunikation müssen definiert und dokumentiert sein. Dies schließt mit ein, wie Ereignisse zeitgerecht eskaliert und die zuständigen Rollen alarmiert werden, inklusive der Auftraggeber (siehe auch Abschnitt 9).

Etwaige BCM-Vorfälle sind zu analysieren. Identifizierte Korrekturbedarfe und Verbesserungsmöglichkeiten müssen durch Maßnahmen behandelt werden. Die Wirksamkeit der umgesetzten Korrekturmaßnahmen muss kontrolliert werden; auf Anfrage des Auftraggebers und unter Wahrung der Geschäftsgeheimnisse des Auftragnehmers ist der Auftraggeber über den Stand und die Wirksamkeit der Umsetzung zu informieren.

8.5 Vorlage von Nachweisen auf Anfrage des Auftraggebers

Die Notfallkonzepte, welche sich mindestens auf den vom Auftragnehmer erbrachten Leistungsbereich beziehen, sind auf Anforderung dem Auftraggeber binnen 2 Wochen vorzulegen. Etwaige Betriebsgeheimnisse, welche in den Notfallkonzepten aufgeführt sind (bspw. detaillierte Wiederanlaufpläne für technische Infrastruktur), können im Ermessen des Auftragnehmers geschwärzt

oder aggregiert werden; der Auftraggeber behält sich etwaige fachliche Rückfragen vor. Dasselbe gilt für Übungspläne und Übungsnachweise für die Notfallkonzepte.

9 Melden von Vorfällen

Der Auftragnehmer muss unverzüglich und ohne schuldhaftes Verzögern den Auftraggeber informieren, sobald Datenschutz- und/oder Sicherheitsvorfälle einschließlich Verdachtsfälle in seinem Zuständigkeitsbereich auftreten, welche den Auftragsgegenstand berühren. Dies gilt insbesondere, da der Auftraggeber gegebenenfalls seiner Informationspflicht gemäß SGB, DSGVO[11] und IT-Sicherheitsgesetz nachkommen muss. Sowohl Auftraggeber als auch Auftragnehmer benennen bei Vertragsschluss Kontaktpunkte für das Melden von Vorfällen.

Entsprechende Analysen und Informationen, inkl. Log-Dateien zum Vorfall, sind dem Auftraggeber auf Anforderung zeitnah und im Rahmen der Bewältigung des Sicherheitsvorfalls nach Möglichkeit zur Verfügung zu stellen. Der Auftraggeber behält sich insbesondere bei Vorfällen eine ad-hoc Überprüfung der Einhaltung der geforderten Sicherheitsmaßnahmen vor sowie eine enge Begleitung der Vorfalls-Analyse. Darüber hinaus hat der Auftragnehmer dem Auftraggeber spätestens auf Anfrage vorzulegen, welche Maßnahmen getroffen wurden, um einen erneuten Angriff oder ein Weiterbestehen der Bedrohungssituation zu beheben.

Folgende Kategorien dienen als Orientierung für Vorfallsarten, welche in jedem Fall eine Meldepflicht an den Auftraggeber auslösen:

- Angriffe auf die IT-Systeme
- Datenverlust
- Relevante Sicherheitslücken[12]
- Widerrechtliche Aktion[13]
- (Anhaltende) Nichtverfügbarkeit
- Besondere sicherheitsrelevante Erkenntnisse

Der Auftraggeber hat das Recht, bei Vorliegen oder Verdacht auf einen Sicherheitsvorfall eine Trennung der IT-Systeme inkl. E-Mail-Verkehr von Auftragnehmer und Auftraggeber zu veranlassen[14].

[11] Die DSGVO sieht bspw. eine Bewertung und Meldepflicht binnen 72 Stunden nach Bekanntwerden vor.

[12] Die Behebung einer schwerwiegenden Sicherheitslücke (CVSS 9-10) sollte dem Auftraggeber mitgeteilt werden, auf Anfrage muss der Auftragnehmer Auskunft zu Betroffenheit und Stand der Behebung erteilen.

[13] Bspw. Verstoß gegen Datenschutzgesetze oder Datenschutz- und IT-Sicherheitsrichtlinien

[14] Eine Trennung der IT-Systeme soll verhindern, dass eine Kompromittierung oder ein aktiver Angriff von den Systemen des Auftragnehmers auf die Systeme des Auftraggebers überspringt (oder umgekehrt). Es handelt sich um eine präventive, je nach eintretendem Vorfall notwendige Maßnahme zum Schutz der IT-Systeme des Auftraggebers und weiterer Beteiligter, die auch bei Verdacht auf einen Sicherheitsvorfall seitens Auftraggeber ergriffen werden kann.

10 Informationssicherheits-Audits

10.1 Regelmäßige Audits durch den Auftragnehmer

Der Auftragnehmer ist verpflichtet, im Umfeld der Leistungserbringung regelmäßig und mindestens jährlich Audits zur IT-Sicherheit und Informationssicherheit durchzuführen. Der Auftragnehmer hat Maßnahmen zur Behebung festgestellter Mängel festzulegen, diese mit dem Auftraggeber abzustimmen und auf Anfrage des Auftraggebers regelmäßig über Fortschritt der Maßnahmenumsetzung sowie der Wirksamkeit der Maßnahmen zu berichten. Hierbei respektiert der Auftraggeber die Wahrung der Betriebsgeheimnisse des Auftragnehmers.

Auf Nachfrage hat der Auftragnehmer dem Auftraggeber Nachweise zu durchgeführten Zertifizierungen und Audits binnen eines Monats zu übermitteln[15]. Aus den Nachweisen geht der Prüfgegenstand und das Ergebnis eindeutig hervor. In Einzelfällen behält sich der Auftraggeber vor, in Abstimmung mit dem Auftragnehmer Einsicht in die beim Auftragnehmer geltende Unterlagen wie bspw. Regelungen zur Informationssicherheit oder Schulungsnachweise zu erhalten.

Penetrationstests sind – als spezifische Form eines technischen Sicherheitsaudits – zusätzlich mindestens jährlich durch den Auftragnehmer und in Abstimmung mit dem Auftraggeber durchzuführen, insbesondere für Systeme, die über einen (öffentlichen) Netzzugang erreichbar sind. Bei Penetrationstests, die den Leistungsgegenstand mittelbar oder unmittelbar betreffen, gilt abweichend zu vorigem Absatz, dass der Abschlussbericht inkl. geplanter Maßnahmen zur Behebung von Mängeln dem Auftraggeber **vollständig[16] und unaufgefordert** vorgelegt werden muss, und zwar spätestens zwei Wochen nach Vorliegen des Abschlussberichts beim Auftragnehmer.

10.2 Audits durch den Auftraggeber

Der Auftraggeber hat jederzeit die Möglichkeit, technische und organisatorische Audits (inkl. Penetrationstests und vor-Ort-Besuche) zur Datensicherheit beim Auftragnehmer durchzuführen oder Dritte damit zu beauftragen. Dies gilt explizit auch für ein (ausgelagertes) Rechenzentrum des Auftragnehmers und die Einbeziehung von Unter-Auftragnehmern. Solche Audits finden für gewöhnlich anlassbezogen statt. Audits dieser Art werden mit angemessenem Vorlauf (abweichende Regelungen bei Sicherheitsvorfällen vgl. Abschnitt 9) vor der Durchführung zwischen Auftraggeber und Auftragnehmer vereinbart.

Führt der Auftraggeber ein Audit zur IT- oder Informationssicherheit beim Auftragnehmer durch, so räumt er dem Auftragnehmer das Recht ein, den Auditbericht auf Anfrage vollumfänglich einzusehen. Ein vom Auftraggeber beauftragtes Audit gilt nicht als Nachweis, dass der Auftragnehmer seine Pflichten zur Durchführung regelmäßiger Sicherheits-Audits erfüllt.

11 Sicherheitskonzept durch den Auftragnehmer

Der Auftragnehmer hat in Abstimmung mit dem Auftraggeber ein Sicherheitskonzept zu entwickeln (vgl. auch § 4 der **02-09-02 Auftragsverarbeitungsvereinbarung**).

---

[15] Hinweis: durch diese Maßnahme soll insbesondere sichergestellt werden, dass der Auftraggeber seinen eigenen Verpflichtungen als auditierte Stelle umfänglich nachkommen kann.

[16] Vollständig, soweit sie mittelbar oder unmittelbar die für den Auftraggeber erbrachten Dienstleistungen betreffen. Punkte, die ausschließlich andere Kunden des Auftragnehmers betreffen, können geschwärzt werden; der Auftraggeber behält sich anlassbezogene Rückfragen und Einsichtnahmen vor.

11.1 Entwicklung, Abstimmung und Implementierung

Das vom Auftragnehmer zu entwickelnde Sicherheitskonzept beschreibt die durch den Auftragnehmer innerhalb der eigenen Systeme, der für den Auftraggeber betriebenen Systeme und Organisation umgesetzten Sicherheitsmaßnahmen und deren Zusammenwirken. Durch die Umsetzung dieser Sicherheitsmaßnahmen wird sichergestellt, dass organisatorische und technische Sicherheitsrisiken, die auf die Systeme und die Organisation des Auftragnehmers wirken, keine Auswirkungen auf die Systeme und Organisation des Auftraggebers haben.

Das Sicherheitskonzept muss vor Verarbeitungsbeginn vorliegen und umgesetzt sein. Es muss durch den Auftraggeber geprüft und freigegeben sein, wobei es bei Bedarf und nach Maßgabe des Auftraggebers durch den Auftragnehmer angepasst werden muss. Auch nach Beginn der Datenverarbeitung wird es fortlaufend durch den Auftragnehmer überprüft und in Abstimmung mit dem Auftraggeber aktualisiert.

11.2 Inhalt des Sicherheitskonzeptes

Der konkrete Inhalt des Sicherheitskonzepts ist abhängig von den spezifischen Anforderungen und Risiken des jeweiligen Systems bzw. Anwendung sowie der Organisation des Auftragnehmers.

Insbesondere ist das Sicherheitskonzept vom Auftragnehmer unter Beachtung der in diesem Dokument („Allgemeine Rahmenbedingungen Informationssicherheit“) gestellten Sicherheitsanforderungen sowie weiterer vertraglicher Vorgaben zur Informationssicherheit und IT-Sicherheit des Auftraggebers an den Auftragnehmer zu erstellen.

425.5Das Sicherheitskonzept enthält unter anderem:

1. Einen allgemeinen Teil:
    a. Planung der Umsetzung der Informationssicherheits-Anforderungen aus diesem Dokument und weiteren vertraglichen Dokumenten
    b. Dokumentation der Umsetzung inkl. bestehender Risiken und Maßnahmen zur Risikosenkung
2. Einen technisch-lösungsspezifischen Teil:
    a. Eine Darstellung der System- und Sicherheitsarchitektur (ggf. als Verweis auf weitere, vom Auftraggeber einsehbare Dokumente)
    b. Gefährdungsbeurteilung der Komponenten
    c. Ableitung von Risiken
    d. Planung von Schutzmaßnahmen zur Risikobehandlung
    e. Dokumentation der Umsetzung der Schutzmaßnahmen

Während der Vertragslaufzeit kann es zu Änderungen in den Vorgaben kommen, die nicht explizit vertraglich vereinbart sind (bspw. bei Verabschiedung neuer Gesetze). Änderungen von größerem Ausmaß werden dem Auftragnehmer schriftlich vom Auftraggeber mitgeteilt und sind ab dann ebenfalls im Sicherheitskonzept und der Umsetzung des Sicherheitskonzepts zu berücksichtigen.

11.3 Überprüfung und Aktualisierung des Sicherheitskonzeptes

Der Auftragnehmer wird das Sicherheitskonzept bei Bedarf, mindestens aber einmal jährlich, überprüfen und überarbeiten, um es den aktuellen Sicherheitsanforderungen sowie Veränderungen der zur Erbringung der Services eingesetzten Systeme, Prozesse und Abläufe anzupassen.

Der Auftragnehmer wird den Auftraggeber über den Status einer Überprüfung unaufgefordert informieren. Der Auftragnehmer wird den Auftraggeber insbesondere bei aufgetretenen Sicherheitsmängeln unaufgefordert und unverzüglich schriftlich informieren.

12 Feinkonzept Informationssicherheitsrisikomanagement durch den Auftragnehmer

Der Auftragnehmer wird ein „Feinkonzept Informationssicherheitsrisikomanagement“ erstellen und mit dem Auftraggeber abstimmen (vgl. **02-04 Prozessrichtlinien** die Prozesse „Manage Informationssicherheit“ und „Manage IT Service Continuity“ sowie in **02-03 Governancemodell** das Gremium „IT Security, Risiko und Compliance Meeting“).

Die Erstellung erfolgt erstmalig während der Transition mit jährlicher Überarbeitung nach Verarbeitungsbeginn. Inhaltlich wird der Auftraggeber insbesondere seine Risiko-Bewertungsklassen zum Schadensausmaß und zur Eintrittswahrscheinlichkeit vorgeben.