

Anlage L4

Informationssicherheit und
Notfallmanagement



Eigentümer:in:

ARGE Online-Sozialwahl 2029

Informationen zum Dokument	
Dokumententitel	Vertragsanlage Informationssicherheit und Notfallmanagement
Autoren	Kai Sonnenwald, Krankenkassen
Eigentümer:in	ARGE Online Sozialwahl 2029
Freigabe durch	ARGE LA

Aktuelle Version		
Version	1.1	
erstellt am	05.06.2026	
Status	☐ Entwurf ☐ In Abstimmung ☒ Final ☐ Final und freigegeben ☐ Archiviert	

Aktualisierungshistorie			
Version	Datum	Beschreibung	Bearbeiter:in
1.0	13.05.2026	Initiale Erstellung	Kai Sonnenwald (TK)
1.1	22.05.2026	Abstimmung zwischen den beteiligten Kassen und entsprechende Überarbeitungen	Kai Sonnenwald (TK) Michael Vaillant (TK) Alexander Umbreit (Barmer) Donald Wedemeyer (KKH) Stefan Hinze (DAK) Knut Woller (DAK) Dirk Krüger (DAK)
1.2	05.06.2026	Ergänzung der Kommentierung der hkk, Anpassung „ARGE“ zu „Krankenkassen“ und „AN“ zu „Auftragnehmer“	Kai Sonnenwald (TK)

Inhaltsverzeichnis

1 Organisatorische Anforderungen	4
1.1 Anforderungen an die Informationssicherheit	4
1.2 Prüfrechte der Krankenkassen	4
1.3 Meldung und Aufklärung von Sicherheitsvorfällen	5
1.4 Informationssicherheitsmanagementsystem	5
1.5 Business Continuity Management	5
1.5.1 Business Continuity Management System	5
1.5.2 Business Continuity Plan	6
1.5.3 Business Continuity Tests	6
1.6 Einsatz von Cloud-Computing	6
1.7 Standorte	6
1.8 Datensicherung und Datenexport	7
1.9 Schulung und Sensibilisierung	7
1.10 Änderung von sicherheitsrelevanten Anforderungen	7
1.11 Pflichten bei Vertragsende	7
2 Technische Anforderungen	8
2.1 Sicherheitsmaßnahmen	8
2.2 Freiheit von Schadsoftware	8
2.3 Systeme zur Angriffserkennung	8
2.4 Benutzerrechtenmanagement	8
2.5 Netzwerksicherheit	8
2.6 Anwendungsschnittstellen	9
2.7 Bestandteile der Software (SBOM)	9
2.8 Anforderungen an Softwareentwicklung	9
2.9 Logging	9
2.10 Patch- und Release-Management	10
2.11 Patch- und Releasemanagement bei Betrieb durch den Auftragnehmer	10
2.12 Schwachstellenmanagement	10
2.13 Verschlüsselung	10
2.14 Datenlöschung	11

1 Organisatorische Anforderungen

1.1 Anforderungen an die Informationssicherheit

Der Auftragnehmer gewährleistet die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten der Krankenkassen und verpflichtet sich, angemessene, geeignete technische und organisatorische Maßnahmen zum Schutz der Daten zu ergreifen, die jeweils dem aktuellen Stand der Technik entsprechen. Eine regelmäßige Anpassung der IT-Systeme und Prozesse an neue Bedrohungen wird vorausgesetzt.

1.2 Prüfrechte der Krankenkassen

Die Krankenkassen sind berechtigt, sich vor Leistungsbeginn und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Die Krankenkassen sind berechtigt, regelmäßig (mindestens monatlich, höchstens täglich) oder anlassbezogen (z.B. Bekanntwerden einer über das Netzwerk ausnutzbaren Schwachstelle oder Nachverfolgung von Härtungsmaßnahmen) nichtinvasive Prüfungen wie Portscans und Aufrufe der Webschnittstellen durchzuführen. Darüber hinaus haben die Krankenkassen das Recht, die Sicherheit der beteiligten Systeme und Prozesse im Rahmen von Assessments zu überprüfen. Insbesondere stimmt der Auftragnehmer zu, dass die Krankenkassen bzw. ein von Ihnen beauftragter Prüfer nach Vorankündigung eigene Penetrationstests durchführen darf.

Auf Anforderung der Krankenkassen legt der Auftragnehmer Nachweise über die regelmäßige Durchführung von Audits, Sicherheitsprüfungen, Penetrationstests und Schwachstellenanalysen vor.

Darüber hinaus haben die Krankenkassen das Recht, die Sicherheit der beteiligten Systeme und Prozesse im Rahmen von eigenen Audits, Sicherheitsprüfungen, Penetrationstests und Schwachstellenanalysen selbst zu überprüfen. Die Krankenkassen sind dazu berechtigt, die Prüfungen durch von ihr beauftragte Prüfer durchführen zu lassen.

Hierzu hat der Auftragnehmer den Krankenkassen bzw. einem von den Krankenkassen beauftragten Prüfer während der normalen Geschäftszeiten Zugang zu den für die Verarbeitung der Daten der Krankenkassen relevanten Verarbeitungssystemen, Einrichtungen sowie zu unterstützenden Unterlagen zu gewähren.

Auf Anforderung der Krankenkassen unterstützt der Auftragnehmer die Krankenkassen bei der Durchführung von Audits, Zertifizierungen und Prüfungen, die im Zusammenhang mit den vertragsgegenständlichen Leistungen durchgeführt werden.

Prüfungen können auch durch Aufsichtsbehörden der Krankenkassen veranlasst werden. Der Auftragnehmer verpflichtet sich, in vollem Umfang mit den für die Krankenkassen zuständigen Aufsichtsbehörden zu kooperieren. Prüfungen finden mit angemessener Vorankündigung für den Auftragnehmer sowie unter Einhaltung der Geheimhaltung statt. Vor Beginn einer solchen Prüfung teilen die Krankenkassen den initialen Prüfungsgegenstand und den geplanten Umfang mit, damit der Auftragnehmer entsprechend disponieren kann. Über Ort, Datum und Ansprechpartner stimmen sich die Parteien ab. Ein Abschlussbericht sowie die daraus abgeleiteten Maßnahmen werden dem Auftragnehmer von den Krankenkassen

innerhalb von 90 Tagen bereitgestellt. Jede Partei trägt die ihr entstehenden Kosten für derartige Prüfungen selbst.

1.3 Meldung und Aufklärung von Sicherheitsvorfällen

Der Auftragnehmer hat einen Prozess zur Erkennung, Meldung und Bearbeitung von Sicherheitsvorfällen und Datenschutzverstößen einzurichten und verpflichtet sich, die Krankenkassen unverzüglich über Vorfälle zu informieren sowie einen detaillierten Bericht über Ursachen, Auswirkungen und Schweregrad des Sicherheitsvorfalls, sowie ergriffene Maßnahmen bereitzustellen. Auch Sicherheitsvorfälle in der vorgelagerten Lieferkette sind den Krankenkassen zu melden. Die Meldung muss unverzüglich an das ARGE-Büro erfolgen unter Berücksichtigung des „Responsible Disclosure“-Verfahrens.

Im Falle eines Sicherheitsvorfalls, bei dem es zu einem potenziellen Datenabfluss oder einer potenziellen Kompromittierung von Daten gekommen sein könnte, verpflichtet sich der Auftragnehmer auf eigene Kosten zu einer qualifizierten forensischen Aufarbeitung des Vorfalls durch einen externen Dienstleister. Der Auftragnehmer hat die Ergebnisse dieser Aufarbeitung der Krankenkassen schnellstmöglich zur Verfügung zu stellen, insbesondere in welchem Umfang Daten von Wahlberechtigten betroffen sind.

Der Auftragnehmer stellt der Krankenkassen auf Anforderung alle erforderlichen Informationen bereit, welche die Krankenkassen zur Erfüllung ihrer Meldepflichten gegenüber Behörden sowie zur Befolgung etwaiger Herausgabepflichten benötigt.

1.4 Informationssicherheitsmanagementsystem

Der Auftragnehmer verpflichtet sich, ein Informationssicherheitsmanagementsystem (ISMS) gemäß ISO/IEC 27001 oder BSI-IT Grundschutz zu implementieren, aufrechtzuerhalten und regelmäßig in angemessener Form zu überprüfen.

Ein entsprechendes, aktuell gültiges, Zertifikat (ISO/IEC 27001) ist zur Angebotsabgabe und fortlaufend mindestens jährlich gegenüber den Krankenkassen nachzuweisen. Bei unterjährigen - für die Krankenkassen relevanten - Änderungen des Zertifikats ist die Krankenkassen unverzüglich zu informieren.

1.5 Business Continuity Management

1.5.1 Business Continuity Management System

Der Auftragnehmer ist verpflichtet, ein vollständig implementiertes, dokumentiertes und betriebenes BCMS gemäß dem Standard BSI 200-4 vorzuhalten. Das BCMS muss die für die Krankenkassen erbrachte Leistung umfassen und mindestens folgende Elemente umfassen und dokumentiert nachweisen:

- eine Business Impact Analyse (BIA)
- eine Risikoanalyse bezogen auf die identifizierten kritischen Ressourcen
- definierte Wiederanlaufzeiten (RTO)
- dokumentierte Notfall- und Wiederanlaufverfahren
- benannte Rollen, inkl. Verantwortlichkeiten und Vertretungsregelungen
- ein Schulungs- und Sensibilisierungskonzept für relevante Mitarbeitende

1.5.2 Business Continuity Plan

Der Auftragnehmer ist verpflichtet, einen Business Continuity Plan (BCP) zu erstellen, der die für die Krankenkassen erbrachten Leistungen umfasst. Der BCP muss mindestens folgende Inhalte enthalten:

- Beschreibung der betroffenen Dienstleistungen für die Krankenkassen
- Identifizierte Störszenarien
- Konkrete Wiederanlaufmaßnahmen je Szenario
- Verbindliche Wiederanlaufzeiten (RTO)
- Kommunikations- und Eskalationsprozesse mit Schnittstellen zu den Krankenkassen
- Abhängigkeiten von Unterauftragnehmern und kritischen Vorlieferanten

Der BCP ist der Krankenkassen nach Vertragsschluss innerhalb von sechs Monaten vorzulegen. Etwaige Schnittstellen der erbrachten Leistung zu den Krankenkassen sind ggf. gemeinsam zwischen dem Auftragnehmer und der Krankenkassen abzustimmen. Für die Krankenkassen relevante Änderungen am BCP sind der Krankenkassen unverzüglich in aktualisierter Fassung zur Verfügung zu stellen.

1.5.3 Business Continuity Tests

Der Auftragnehmer ist verpflichtet, die im BCP definierten Maßnahmen mindestens einmal jährlich durch strukturierte Tests oder Übungen zu überprüfen.

Die Tests müssen mindestens folgende Kriterien erfüllen:

- Durchführung anhand realitätsnaher Szenarien
- Einbeziehung der für die Krankenkassen relevanten Dienstleistungen
- Bewertung der Einhaltung der definierten Wiederanlaufzeiten.

Über jeden Test ist ein Protokoll zu erstellen, das mindestens enthält:

- Datum, Art und Umfang des Tests,
- getestete Szenarien
- erzielte Wiederanlaufzeiten
- festgestellte Abweichungen
- definierte Korrekturmaßnahmen inkl. Umsetzungsfristen.

Das Protokoll ist der Krankenkassen spätestens vier Wochen nach Durchführung unaufgefordert zur Verfügung zu stellen.

1.6 Einsatz von Cloud-Computing

Sofern der Auftragnehmer im Rahmen der Leistungserbringung Cloud-Computing Dienste nutzt, sind C5-testierte Cloud-Computing Dienste zu nutzen. Zum Zeitpunkt der Wahldurchführung muss ein gültiges C5-Testat gemäß der dann geltenden Version des C5-Standards vorliegen. Das Testat muss auf Verlangen der Krankenkassen zum Nachweis und zur Prüfung vorgelegt werden.

1.7 Standorte

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland

bedarf der vorherigen Zustimmung der Krankenkassen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

1.8 Datensicherung und Datenexport

Der Auftragnehmer ist verpflichtet, in regelmäßigen Abständen Datensicherungen vorzunehmen. Zudem muss der Auftragnehmer in angemessener Frist eine Wiederherstellung von Daten aus einem Backup, auf den von den Krankenkassen gewünschten vorhandenen Stand vornehmen können.

Der Auftragnehmer muss über praxiserprobte Backup- und Restore-Konzepte verfügen und diese der Krankenkassen auf Anforderung nachweisen.

Die Leistung ist so auszugestalten, dass die Krankenkassen jederzeit selbstständig oder, soweit dies aus technischen Gründen nicht möglich ist, mit Unterstützung durch den Auftragnehmer ihre Daten in einem marktüblichen Austauschformat exportieren kann. Damit muss auch der Export von bestimmten Teilen der Daten der Krankenkassen möglich sein. Soweit die Daten verschlüsselt sind, ist diese Pflicht nur dann erfüllt, wenn die Krankenkassen auch über den Schlüssel verfügt. Für den Export der Daten und deren Sicherung nach dem Export ist die Krankenkassen verantwortlich.

1.9 Schulung und Sensibilisierung

Der Auftragnehmer ist verpflichtet, Mitarbeitende regelmäßig über Informationssicherheitsanforderungen zu schulen und sicherzustellen, dass die für die Leistungserbringung eingesetzten Mitarbeitenden die notwendigen Kenntnisse zur Einhaltung der vertraglich vereinbarten Sicherheitsstandards besitzen.

1.10 Änderung von sicherheitsrelevanten Anforderungen

Sofern sich sicherheitsrelevante Anforderungen, auf die im Rahmen dieses Vertrages verwiesen wird, während der Vertragslaufzeit ändern, wird der Auftragnehmer auch die neuen bzw. geänderten Anforderungen unaufgefordert innerhalb angemessener Frist erfüllen, spätestens ab Inkrafttreten oder gegebenenfalls innerhalb der Übergangsfristen.

Sofern dem Auftragnehmer eine Erfüllung der neuen Anforderungen nicht möglich ist, teilt er dies der Krankenkassen unverzüglich, in jedem Fall innerhalb der vom Gesetzgeber vorgesehenen Umsetzungsfrist, ab Veröffentlichung der neuen Anforderung mit.

1.11 Pflichten bei Vertragsende

Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch die Krankenkassen – spätestens mit Beendigung des Vertrages – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Daten, erstellte Verarbeitungs- und Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, der Krankenkassen auszuhändigen oder nach vorheriger Zustimmung entsprechend der Anforderungen zur Datenlöschung zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

2 Technische Anforderungen

2.1 Sicherheitsmaßnahmen

Der Auftragnehmer muss alle zumutbaren und geeigneten technischen und organisatorischen Maßnahmen ergreifen, die einen unbefugten und missbräuchlichen Zugriff auf die eingesetzten IT-Systeme, Anwendungen, zugehörige Komponenten sowie zugehörige Daten unterbinden. Die getroffenen Maßnahmen müssen dabei dem aktuellen Stand der Technik entsprechen.

Der Einsatz von kritischen Komponenten deren Einsatz gemäß BSIG §41 vom BMI untersagt wurde, ist nicht erlaubt. Zur Vertragslaufzeit betroffene Komponenten müssen unverzüglich durch den Auftragnehmer ausgetauscht werden.

Sollten sich aufgrund neuer Erkenntnisse oder Bedrohungen Sicherheitslücken ergeben, so muss der Auftragnehmer diese unverzüglich den Krankenkassen anzeigen und sie durch geeignete Maßnahmen beseitigen. Sofern die Maßnahmen die Verfügbarkeit, der für die Krankenkassen zur Verfügung gestellten Dienste beeinflussen, muss der Auftragnehmer diese mit den Krankenkassen abstimmen.

2.2 Freiheit von Schadsoftware

Alle Bestandteile der erbrachten Leistung müssen frei von Schadsoftware sein. Der Auftragnehmer muss dies durch geeignete Maßnahmen sicherstellen. Der Auftragnehmer muss insbesondere beteiligte IT-Systeme und Software mittels eines marktgängigen und aktuellen Scanners oder mindestens gleichwertiger Technologie prüfen.

2.3 Systeme zur Angriffserkennung

Der Einsatz von Systemen zur Angriffserkennung entsprechend der „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“ des BSI in der jeweils aktuell gültigen Version ist seitens des Auftragnehmers verpflichtend.

2.4 Benutzerrechtenmanagement

Der Auftragnehmer hat sicherzustellen, dass der Zugriff auf Systeme, Anwendungen und Daten/Informationen ausschließlich autorisierten Personen nach dem Prinzip der minimalen Rechtevergabe gewährt wird und geeignete technische Maßnahmen wie Zwei-Faktor- bzw. Multi-Faktor-Authentifizierung implementiert sind. Der Auftragnehmer muss für sicherheitsrelevante Prozesse das Vier-Augen-Prinzip umsetzen. Die vorhandenen Rollen und Rechte sind in einem Berechtigungskonzept zu beschreiben und auf Wunsch der Krankenkassen vorzulegen.

2.5 Netzwerksicherheit

Der Auftragnehmer stellt sicher, dass er seine angebotenen Dienste netzwerkseitig angemessen schützt. Dazu gehört eine Segmentierung der Netzwerke entsprechend der fachlichen Notwendigkeit und die Etablierung eines feingranularen Regelwerks zur Beschränkung des Netzwerkverkehrs auf die zur Leistungserbringung notwendigen Dienste.

2.6 Anwendungsschnittstellen

Der Auftragnehmer stellt sicher, dass externe Schnittstellen (APIs) der bereitgestellten Anwendungen angemessen gegen unbefugte Nutzung geschützt sind.

2.7 Bestandteile der Software (SBOM)

Der Auftragnehmer ist zur Lieferung einer SBOM (Software Bill of Materials) für die eingesetzte Software verpflichtet. SBOM ist eine formale, strukturierte Aufzeichnung, die die Artefakte einer Software identifiziert und ihre Beziehungen untereinander und zu anderer Software/anderen Artefakten beschreibt. Diese muss für jede Standardsoftware und jeden Bestandteil gemäß BSI TR-03183-2 bereitgestellt werden.

Anforderungen an die Software-Entwicklung?

2.8 Anforderungen an Softwareentwicklung

Der Auftragnehmer ist verpflichtet im Rahmen der Softwareentwicklung des angebotenen Online-Wahlsystems folgende Aspekte zu beachten:

- Im Rahmen der Softwareentwicklung sind die Prämissen Least Functionality, Security by Design und Privacy by Design zu berücksichtigen.
- Es muss ein Betriebshandbuch für die entwickelte Anwendung bereitgestellt werden.
- Der Prüfkatalog der deutschen Datenschutzaufsichtsbehörden im Bereich der App-Entwicklungen und die BSI TR-03161 sind zu berücksichtigen.
- In eigenentwickeltem Code sind Code-Qualitätsstandards zu berücksichtigen.
- Es müssen standardmäßig und strukturiert im Rahmen des Entwicklungsprozesses Modul-, Integrations-, Sicherheits- und Abnahmetests durchgeführt und protokolliert werden. Testfälle und Testergebnisse sind zu dokumentieren und sind nach Wunsch der Krankenkassen bereitzustellen.
- Bei eigenentwickeltem Code sind Verfahren zur Schwachstellenerkennung anzuwenden.
- Bei der Nutzung von Drittanbieterkomponenten sind Verfahren zur Schwachstellenerkennung anzuwenden.
- Es muss ein Change-Management inkl. Freigabeverfahren vorhanden sein.
- Es muss ein Problem-Management inkl. Lösungen und Maßnahmen zur künftigen Prävention vorhanden sein.
- Vor einer Produktivsetzung der entwickelten Software muss ein Penetrationstest durchgeführt werden. Eventuelle Befunde müssen behoben werden und die Ergebnisse sind der Krankenkassen mitzuteilen.

2.9 Logging

Zugriffe auf sensible oder sozialversicherungsrechtliche Daten sowie administrative Zugriffe und das Starten von Batch-Prozessen müssen mittels Logging protokolliert werden.

Das Logging soll mittels der Logging Facility der jeweiligen Plattform (bspw. Windows-Eventlog, Syslog) erfolgen. Sofern die Logging Facility der jeweiligen Plattform nicht verwendet wird, müssen Logeinträge in Dateien oder Datenbanken gespeichert werden.

Logeinträge müssen maschinell auswertbar sein. Über das Format der Logeinträge muss ab Leistungsbeginn eine vollständige und verständliche Dokumentation geliefert werden.

Sämtliche Logeinträge müssen einen Zeitstempel enthalten. Der Zeitstempel muss auf der Betriebssystemzeit beruhen oder es muss anderweitig sichergestellt werden, dass die

Abweichung zu einer offiziellen Zeitquelle (z. B. einem NTP-Server) weniger als 3 Sekunden beträgt. Sofern die Logeinträge nicht in von Menschen lesbarer und verständlicher Form für Revisionszwecke vorliegen, müssen entsprechende Aufbereitungsprogramme zur Verfügung gestellt werden. Logdaten müssen vor unberechtigten Zugriffen geschützt sein.

2.10 Patch- und Release-Management

Jegliche eingesetzte oder selbst entwickelte Software muss gepflegt werden. Dazu gehört eine regelmäßige Anpassung an die aktuelle Bedrohungslage durch Schwachstellen und neue Anforderungen. Der Auftragnehmer informiert die Krankenkassen selbstständig und ohne Aufforderung schriftlich über neue Versionen und Patches.

Sicherheitsrelevante Patches auf Plattform- und Datenbankebene müssen spätestens 2 Wochen nach deren genereller Verfügbarkeit unterstützt werden. Service Packs und neue Maintenance Level auf Plattform- und Datenbankebene müssen spätestens 3 Monate nach der generellen Verfügbarkeit unterstützt werden. Neue Releases auf Plattform- und Datenbankebene müssen spätestens 12 Monate nach deren genereller Verfügbarkeit unterstützt werden. Sofern Anwendungskomponenten auf Windows-Clientsystemen vorgesehen sind, müssen diese neue Windows-Funktionsupdates innerhalb von 6 Monaten nach genereller Verfügbarkeit unterstützen.

2.11 Patch- und Releasemanagement bei Betrieb durch den Auftragnehmer

Bei einem Betrieb von IT-Komponenten durch den Auftragnehmer muss dieser über einen Patch-Management-Prozess verfügen, dass alle von ihm eingesetzten Systeme, Systemkomponenten und Entwicklungswerkzeuge jeweils auf einem aktuellen Versionsstand und insbesondere frei von Schwachstellen sind. Der Auftragnehmer muss sicherstellen, dass je nach Risiko für die Anwendung (bewertet durch den Auftragnehmer) Sicherheitspatches - innerhalb von 1-5 Arbeitstagen nach Veröffentlichung des Patches eingespielt werden.

2.12 Schwachstellenmanagement

Der Auftragnehmer betreibt ein aktives Schwachstellenmanagement. Es werden regelmäßig geplant Schwachstellenscans auf den eingesetzten IT-Systemen durchgeführt und die Ergebnisse in einem risikobasierten Ansatz zur Verbesserung der Sicherheitsmaßnahmen verwendet.

Wenn der Auftragnehmer Leistungen im Rahmen des öffentlichen Internetauftritts der Krankenkassen erbringt (Nutzung Public IPs, (Sub-)Domänen) ist die Leistung an das Schwachstellenmanagement der Krankenkassen anzubinden.

2.13 Verschlüsselung

Alle Daten der Krankenkassen müssen sowohl bei der Speicherung als auch beim Transport verschlüsselt werden.

Sofern in der Anwendung Verschlüsselungen eingesetzt werden, müssen die verwendeten Verschlüsselungsalgorithmen zur aktuellen Fassung der BSI TR-02102-1 konform sein. Sofern Verschlüsselungsalgorithmen im direkten Umfeld von qualifizierten elektronischen Signaturen nach dem bundesdeutschen Signaturgesetz eingesetzt werden, müssen sie sich nach den Veröffentlichungen der Bundesnetzagentur im Bundesanzeiger richten.

Verschlüsselungsverfahren müssen vor Ablauf des genehmigten Verwendungsdatums durch aktuelle Verfahren ersetzt werden.

Sofern TLS zur Transportverschlüsselung eingesetzt wird, muss der Auftragnehmer sich bei der Wahl von TLS-Version(en) und der einzusetzenden Cipher-Suites an die Empfehlungen der jeweils aktuellen Fassung der BSI TR-02102-2 halten. Der Auftragnehmer muss die von ihm gewählte Konfiguration mindestens jährlich gegen die Vorgaben des BSI abgleichen und bei Bedarf anpassen.

Sollen Zufallszahlen in der Anwendung verwendet werden, so müssen diese – dem Anwendungszweck entsprechend – hinreichend zufällig sein. Als Informationsquelle für zulässige Zufallszahlengeneratoren kann ebenfalls die aktuelle Technische Richtlinie TR-02102-1 des BSI dienen.

2.14 Datenlöschung

Bei der Verwendung von SaaS werden Storage-Komponenten (die zur persistenten Speicherung von Daten verwendet werden) bei Außerbetriebnahme einer Appliance, des Services und bei der Beendigung des Vertrages gelöscht. Die Löschung einer Speicherkomponente entspricht einer physischen Vernichtung. Die Löschung aller virtuellen Ressourcen muss in einem Protokoll dokumentiert werden. Dieses Protokoll muss der TK zur Verfügung gestellt werden. Gelöschte Speicherressourcen dürfen nicht wiederherstellbar sein.

Bei der Außerbetriebnahme einer Appliance, bei Austausch von Hardware-Komponenten sowie bei der Beendigung eines Vertrages und vor der Wiederverwendung von Speichermedien durch andere Kunden des Auftragnehmers, müssen alle permanent speichernden Datenträger sicher vernichtet oder sicher gelöscht werden. Eine Weitergabe oder Rückgabe an Dritte, ausgenommen zur professionellen Löschung bzw. Vernichtung, darf nicht stattfinden. Der Auftragnehmer muss über die erfolgte Vernichtung/Löschung ein Protokoll anfertigen, aus dem hervorgeht, wann und mittels welchen Verfahrens die Datenträger vernichtet/gelöscht wurden. Der Auftragnehmer muss der Krankenkassen das Protokoll auf Anforderung zur Verfügung stellen.

Für Datenträger mit folgenden Kriterien muss eine Vernichtung erfolgen. Löschen ist unzulässig bei defekten Datenträgern und Wechselmedien (USB-Sticks, Speicherkarten, etc.).

Eine Vernichtung muss gemäß folgender Vorgaben oder gleich-/höherwertiger Verfahren erfolgen:

- Festplatten (HDD): DIN 66399-2, mindestens Stufe H-4
- Solid State Disks (SSD), Hybridfestplatten (SSHD), Wechselmedien: DIN 66399-2, mindestens Stufe E-4

Bei allen funktionsfähigen, verschlüsselten magnetischen Datenträgern kann eine elektronische sichere Löschung durchgeführt werden. Dabei muss die Löschung auf dem gesamten Datenträger nach dem nachfolgenden Löschverfahren erfolgen:

1. Löschfunktion des Laufwerks (ATA "Secure Erase")
2. DoD 5220.22-M (ECE) bzw. gleich-/höherwertig
3. Löschfunktion des Laufwerks (ATA "Secure Erase")

Bei allen funktionsfähigen, verschlüsselten halbleiterbasierten Datenträgern kann eine elektronische sichere Löschung durchgeführt werden. Dabei muss die Löschung auf dem gesamten Datenträger nach einem der nachfolgenden Lösungsverfahren erfolgen:

- Verfahren 1:
 1. Löschfunktion des Mediums (ATA-"Secure-Erase")
 2. Überschreiben des gesamten Speichers
 3. Löschfunktion des Mediums (ATA-"Secure-Erase")
- oder Verfahren 2:
 1. Löschen des Schlüssels für die Festplattenverschlüsselung im TPM-Chip
 2. Überschreiben des gesamten Speichers
 3. Löschen des Schlüssels für die Festplattenverschlüsselung im TPM-Chip