## Anhang 2 zu Anlage 1 – Anforderungen Informationssicherheit AOK PLUS

| | |
|---|---|
| Muss | Ist zu erfüllen |
| Soll | Es kann begründet abgewichen/nicht erfüllt werden |
| | |
| | |
| **Bezeichnung** | **Inhalt / Anforderung** |
| MUSS: Nachweis eines Notfallplans für den Ausfall der Dienstleistung | Verantwortliche müssen für den Falle des Ausfalls der Dienstleistung (voraussichtliche Dauer übersteigt den RTO(die Wiederanlaufzeit) des Prozesses) einen Notfallplan erstellen und vertesten.<br><br>Diese Anforderung stellt sicher, dass ein Notfallplan vorliegt, falls ein Dienstleister (DL) ausfällt oder seine Leistungen nicht mehr erbringen kann. Der Plan beschreibt, wie der Geschäftsbetrieb trotz des Ausfalls weitergeführt oder schnellstmöglich wiederhergestellt werden kann. So wird gewährleistet, dass kritische Prozesse abgesichert sind und Ausfallzeiten sowie Risiken für das Unternehmen minimiert werden. |
| MUSS: Pflicht zur Ursachenanalyse bei Abweichungen von Vereinbarungen | Dienstleister müssen bei einer festgestellten Nichtkonformität oder Abweichung von den vertraglich vereinbarten Verpflichtungen eine Überprüfung und Ursachenanalyse gemeinsam mit der AOK PLUS durchführen.<br><br>Diese Anforderung stellt sicher, dass bei jeder Abweichung von vertraglichen oder internen Vereinbarungen systematisch untersucht wird, warum es zu der Abweichung gekommen ist. Die Ursachenanalyse dient dazu, die eigentlichen Gründe, etwa Prozessfehler, technische Probleme oder mangelnde Kommunikation, zu identifizieren. Auf dieser Basis können gezielte Korrektur- und Vorbeugungsmaßnahmen entwickelt werden, um ähnliche Abweichungen künftig zu vermeiden und die Qualität sowie Zuverlässigkeit der Dienstleistungen zu sichern. |

| | |
|---|---|
| MUSS: Rückgabe oder Vernichtung von Zugangsdaten, Zugangsmittel und Authentifizierungsmitteln | Alle Dienstleister müssen die ausgehändigten Zugangsdaten, Zugangsmittel, Authentifizierungsmechanismen und Hardware, zurückgeben oder vernichten.Diese Anforderung stellt sicher, dass Zugangsdaten, Passwörter, Schlüssel oder andere Authentifizierungsmittel nach der Beendigung einer Nutzung oder eines Beschäftigungsverhältnisses ordnungsgemäß zurückgegeben oder sicher vernichtet werden. Dadurch wird verhindert, dass unbefugte Personen weiterhin Zugriff auf Systeme, Daten oder Räume erhalten.Die Rückgabe oder Vernichtung ist nachzuweisen. |
| MUSS: Sicherstellung des autorisierten Zugriffs und der Rechtevergabe | Für Dienstleister mit Zugang zu nicht öffentlichen Informationen muss sichergestellt werden, dass der Zugriff auf Informationen und Systeme ausschließlich berechtigten Personen vorbehalten ist und nach dem Prinzip der minimalen Rechte (Need-to-Know-Prinzip) erfolgt.Diese Anforderung stellt sicher, dass nur berechtigte Personen auf Systeme, Anwendungen oder Daten zugreifen können. Die Rechtevergabe erfolgt gezielt nach dem Prinzip der minimalen Berechtigung, sodass jede Person nur die Zugriffsrechte erhält, die sie tatsächlich für ihre Aufgaben benötigt. Dadurch werden unbefugte Zugriffe verhindert und die Sicherheit sowie Integrität der Informationen gewährleistet. |
| MUSS: Unterzeichnung von Vertraulichkeitsvereinbarungen | Dienstleister mit Zugang zu nicht öffentlichen Informationen müssen vertraglich verpflichtet werden, strikte Vertraulichkeit zu wahren. Es müssen entsprechende Vertraulichkeitsvereinbarungen der AOK PLUS unterzeichnet und dokumentiert werden.Diese Anforderung stellt sicher, dass Personen, die Zugriff auf interne Informationen oder sensible Daten erhalten, eine Vertraulichkeitsvereinbarung (Non-Disclosure Agreement, NDA) unterzeichnen. Dadurch verpflichten sie sich, die Informationen nur für die vorgesehenen Zwecke zu nutzen und nicht an unbefugte Dritte weiterzugeben. Insbesondere werden damit die Anforderungen des GeschGehG - Gesetz zum Schutz von Geschäftsgeheimnissen <https://www.gesetze-im-internet.de/geschgehg/BJNR046610019.html> erfüllt. |
| SOLL: Backup und Redundanz | IT-Dienstleister sollen nachweisen, dass Sie ihre Systeme so absichern, dass Datenverlust oder Ausfälle möglichst vermieden werden. Dazu gehören zum Beispiel regelmäßige Datensicherungen (Backups), doppelte Systeme oder Server (Redundanzen) und andere Sicherheitsvorkehrungen. So bleibt der Betrieb auch bei technischen Problemen stabil, und wichtige Daten können im Notfall schnell wiederhergestellt werden. |

| | |
|---|---|
| SOLL: Betrieb von Software mit Sicherheitsupdates | IT-Dienstleister sollen nur Softwarelösungen betreiben, welche weiterhin mit Sicherheitsupdates versorgt werden. Diese Sicherheitsupdates sollen durch die IT-Dienstleister in angemessener Zeitspanne eingespielt werden. Endet die Versorgung mit Sicherheitsupdates und Support, sollen IT-Dienstleister den Betrieb einstellen.Diese Anforderung stellt sicher, dass Systeme oder Anwendungen nicht weiter betrieben werden, wenn für sie keine Sicherheitsupdates mehr verfügbar sind oder der Hersteller den Support eingestellt hat. Ohne solche Updates entstehen Sicherheitslücken, die Angriffe erleichtern können. Durch die Betriebseinstellung wird das Risiko für Datenverlust, Systemausfälle oder Sicherheitsvorfälle minimiert. |
| SOLL: Einhaltung der Anforderungen aus Business Impact Analyse (BIA) | Dienstleister sollen * die maximal tolerierbare Ausfallzeit (MTPD) * die Wiederanlaufzeit (RTO) * und den maximal tolerierbaren Datenverlust (RPO)basierend auf der Business Impact Analyse (BIA) der Prozesse der Auftraggeberin einhalten.Eine bei der AOK PLUS durchgeführte Business Impact Analyse (BIA) untersucht, wie kritisch ihre einzelnen Prozesse sind und wie lange ein Ausfall maximal dauern darf, ohne großen Schaden zu verursachen. Auf dieser Grundlage werden bei der AOK PLUS MTPD, RPO und RTO festgelegt.Dienstleister sollen ihre eigenen Notfall- und Wiederherstellungsmaßnahmen so planen und umsetzen, dass diese Zeiten sicher eingehalten werden - damit die wichtigsten Geschäftsprozesse der Auftraggeberin auch im Ernstfall zuverlässig weiterlaufen können. |
| SOLL: Einhaltung des Stands der Technik | Alle Dienstleister sollen dem aktuellen Stand der Technik entsprechende Maßnahmen zur Wahrung der Informationssicherheit (Vertraulichkeit, Verfügbarkeit, Integrität (inkl. Authentizität)) umsetzen. Das umfasst z.B. technische Sicherheitsvorgaben, organisatorische Abläufe und Schutzmaßnahmen, die allgemein anerkannt und bewährt sind. Ziel ist, Risiken wie Datenverlust, Ausfälle oder Sicherheitsvorfälle möglichst zu minimieren und die Qualität sowie Sicherheit der erbrachten Leistungen dauerhaft zu gewährleisten. |

| | |
|---|---|
| SOLL: Einräumung von Audit-Rechten zur Überprüfung der Anforderungserfüllung | Alle Dienstleister sollen ein Audit-Recht einräumen, bei welchem die Auftraggeberin oder ein durch sie beauftragter Dritter die Erfüllung der gestellten Anforderungen regelmäßig und anlassbezogen überprüfen kann.<br><br>Solche Audits können organisatorische Abläufe, Sicherheitsmaßnahmen, Prozesse oder technische Systeme betreffen. Ziel ist, Transparenz zu schaffen, Risiken frühzeitig zu erkennen und sicherzustellen, dass die vereinbarten Standards und Vorschriften tatsächlich umgesetzt werden. |
| SOLL: Einsatz von sicheren Verschlüsselungstechnologien und Übertragungsverfahren | Alle IT-Dienstleister sollen Verschlüsselungstechnologien sowie sichere und für den jeweiligen Einsatzzweck geeignete Übertragungsverfahren nach dem Stand der Technik einsetzen.Diese Anforderung stellt sicher, dass Informationen während der Speicherung und Übertragung geschützt sind. Sichere Übertragungsverfahren verhindern, dass Informationen abgefangen oder manipuliert werden. Damit werden Vertraulichkeit und Integrität sensibler Informationen gewährleistet. |
| SOLL: Löschung nicht öffentlicher Informationen | Der Dienstleister mit Zugang zu nicht öffentlichen Informationen sollte in der Lage sein, nach Beendigung des Vertragsverhältnisses nicht öffentliche Informationen gemäß dem Stand der Technik (z.B. DIN 66399 und ISO/IEC 21964) zu löschen und entsprechende Nachweise darüber zu erbringen.Diese Anforderung stellt sicher, dass nicht öffentliche gelöscht werden, sobald sie nicht mehr benötigt werden oder gesetzliche Aufbewahrungsfristen abgelaufen sind. Dadurch wird das Risiko von unbefugtem Zugriff, Datenmissbrauch oder Informationsverlust minimiert und die Einhaltung von Datenschutz- und Sicherheitsanforderungen gewährleistet. |
| SOLL: Nachweis eines Sicherheitskonzepts | Dienstleister müssen ein Sicherheitskonzept für die sichere Erbringung der Dienstleistung für die AOK PLUS vorlegen. Dieses Sicherheitskonzept muss dokumentiert, umgesetzt, regelmäßig überprüft, sowie kontinuierlich verbessert werden. Diese Anforderung stellt sicher, dass für Systeme, Anwendungen oder Prozesse ein dokumentiertes Sicherheitskonzept vorliegt. Das Konzept beschreibt, welche Schutzmaßnahmen zur Wahrung von Vertraulichkeit, Integrität und Verfügbarkeit der Informationen umgesetzt werden. Der Nachweis dient dazu, zu belegen, dass Risiken systematisch berücksichtigt und angemessene Sicherheitsvorkehrungen getroffen werden. |

| | |
|---|---|
| SOLL: Nachweispflicht eines C5-Testats für Cloud Dienste mit Zugang zu Sozial- oder Gesundheitsdaten | Cloud/*aaS-Dienstleister mit Zugang zu Sozial- oder Gesundheitsdaten müssen ein C5-Testat (Typ 2) vorlegen, um die Einhaltung der Anforderungen an die Informationssicherheit nachzuweisen (siehe § 393 SGB 5 - Einzelnorm <https://www.gesetze-im-internet.de/sgb_5/__393.html>). Diese Anforderung stellt sicher, dass Cloud-Dienste, die Zugriff auf Sozial- oder Gesundheitsdaten haben, ein gültiges C5-Testat nachweisen. Das C5-Testat ist ein Prüfsiegel des Bundesamts für Sicherheit in der Informationstechnik (BSI) und bestätigt, dass der Cloud-Anbieter bestimmte Sicherheitsanforderungen erfüllt. Der Nachweis dient dazu, die Sicherheit sensibler Daten zu gewährleisten und Compliance-Anforderungen einzuhalten.Hinweis: Bitte beachten Sie die Hinweise bzgl. der Verordnung über gleichwertige Sicherheitsnachweise zum C5-Standard für Cloud-Computing-Dienste: C5GleichwV - Verordnung über gleichwertige Sicherheitsnachweise zum C5-Standard für Cloud-Computing-Dienste im Gesundheitswesen <https://www.gesetze-im-internet.de/c5gleichwv/BJNR05B0A0025.html>Die Anforderung kann begründet ausgeschlossen werden. Nutzen Sie hierfür das Hilfewerkzeug im Anhang.BSI Anforderung <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/UPK/upk-exit-strategie-cloud-dienstleistungen.html> |