



Informationssicherheit

Dienstleistungsrichtlinie

Inhalt und Umfang dieses Dokumentes

Das vorliegende Dokument enthält die Regelungen zur Auslagerung von informationssicherheitsrelevanten (IT-)Dienstleistungen an externe Dienstleister im Bereich der kritischen Dienstleistung *stationäre medizinische Versorgung* (kDL) im Universitätsklinikum Augsburg.

Verantwortlichkeiten und grafische Prozessbeschreibungen werden in Anlagen dargestellt.

Vereinbarung zum Dokument

Die in diesem Dokument enthaltenen Informationen und Ergebnisse einschließlich der enthaltenen Anlagen sind urheberrechtlich geschützt. Eine Verwendung außerhalb des Universitätsklinikums Augsburg ist nur nach vorheriger Zustimmung zulässig.

Ferner gilt dies für die Übernahme der vorgeschlagenen Vorgehensweise, die Einsichtnahme Dritter, sowie die Vervielfältigung, Bearbeitungen, Übersetzungen, Mikroverfilmung und die Einspeicherung und Verarbeitung in elektronischen, nachrichtentechnischen oder optischen Systemen.

Betrifft: Alle Mitarbeiter des Universitätsklinikum Augsburg, externe Dienstleister sowie weitere Dritte mit Zugriff auf Informationswerte des UKA im Bereich der kritischen Dienstleistung	
Klassifikation: vertraulich (Mitarbeiter UKA sowie externe Vertragspartner)	
Erst-Erstellung am: 09.08.2021	Stabsstelle Recht, Datenschutz und Informationssicherheit
	Fachliche Prüfung: _____gez._____ Markus Hoefer (HZ)
Freigabe ab: 10.08.2021	Freigabe durch: _____gez._____ stellv. Kaufm. Direktorin

Dienstleistungsrichtlinie

Inhaltsverzeichnis

1.	Einleitung	2
1.1.	Zielsetzung	2
1.2.	Abgrenzung	2
1.3.	Geltungsbereich und Verstöße	3
2.	Übergeordnete Rahmenbedingungen.....	3
3.	Auswahl eines Dienstleisters	3
4.	Vertragsspezifische Regelungen	4
5.	Regelungen zum Notfallmanagement.....	5
6.	Inkrafttreten	6

Hinweise:

In diesem Dokument wird ausschließlich die männliche Anredeform verwendet, sie gilt aber in gleicher Form für alle Geschlechter.

1. Einleitung

1.1. Zielsetzung

Diese Sicherheitsrichtlinie konkretisiert die Anforderungen hinsichtlich einer Auslagerung von sicherheitsrelevanten Diensten – insbesondere IT-Diensten – an externe Stellen/ Dritte, um dabei ein angemessenes Sicherheitsniveau zu gewährleisten.

1.2. Abgrenzung

Diese Sicherheitsrichtlinie bezieht sich lediglich auf die Auslagerung von sicherheitsrelevanten Diensten. Dies betrifft die Auslagerung von Tätigkeiten oder Aufgaben, wenn die folgenden Bedingungen alle erfüllt sind:

- Die Bindung an den Dienstleister erfolgt auf längere Zeit (nicht nur einmalige Beschaffung) und
- durch die Dienstleistung kann die Informationssicherheit der klinischen Applikationen beeinflusst werden und
- im Rahmen der Dienstleistung erbringt der Dienstleister auch regelmäßig nennenswerte Sicherheitsmanagement-Tätigkeiten oder realisiert Sicherheitsmaßnahmen, die die Patientensicherheit und oder den Betrieb der kDL gefährden.

1.3. Geltungsbereich und Verstöße

Diese Sicherheitsrichtlinie gilt für alle Vertragspartner des Universitätsklinikums Augsburg (UKA), die unter den Geltungsbereich fallen und ist bei der Gestaltung von Auslagerungs-Vorhaben zugrunde zu legen, wenn Dienstleistungen im Bereich der Informationsverarbeitung betroffen sind.

Bereits vor jeder Auslagerungs-Entscheidung sind dabei IT- und Informationssicherheitsaspekte zu bedenken und bei einer Ausschreibung/ der Auswahl eines Dienstleisters zu berücksichtigen. Diese Sicherheitsrichtlinie ist gegenüber dem Dienstleister an den die Auslagerung erfolgen soll (im Folgenden als Dienstleister bezeichnet) als Prüfungsgrundlage zu nutzen und den Verträgen mit Dienstleistern zugrunde zu legen.

2. Übergeordnete Rahmenbedingungen

Aus der Informationssicherheitsrichtlinie des UKA ergeben sich die folgenden Rahmenbedingungen, welche bei der Auslagerung von sicherheitsrelevanten Diensten zu berücksichtigen sind:

- Sofern Dienstleistungen an externe Stellen/Dritte ausgelagert werden, müssen konkrete Sicherheitsanforderungen in den Service Level Agreements durch das UKA vorgegeben werden.
- Die Berücksichtigung der rechtlichen Aspekte muss gewährleistet sein und nachgewiesen werden.
- Das uneingeschränkte Recht auf Kontrolle der Erfüllung dieser Anforderungen muss festgelegt werden.
- Für umfangreiche oder komplexe Auslagerungs-Vorhaben muss ein detailliertes Sicherheitskonzept durch den Auslagernden mit konkreten Maßnahmenvorgaben erstellt werden.
- Es muss in jedem Fall gewährleistet sein, dass bezüglich der ausgelagerten Dienste beim Dienstleister das gleiche Sicherheitsniveau erreicht wird, welches auch bei interner Realisierung durch den Auftraggeber erforderlich ist und erreicht worden wäre. Zertifikate anerkannter Normen werden akzeptiert.

3. Auswahl eines Dienstleisters

Es ist selten Erfolg versprechend, eine Geschäftsbeziehung lediglich auf Verträgen und Regressansprüchen zu begründen. Daher ist der Dienstleister sorgfältig auszuwählen und eine vertrauensvolle und kooperative Zusammenarbeit anzustreben.

Bei der Auswahl ist zu prüfen, ob der Auftragnehmer als makellos, unbescholten und unbestechlich einzuschätzen ist (Zuverlässigkeit) und ob ein ernsthaftes und fachkundiges Betreiben der Dienstleistung gewährleistet ist (Seriosität).

Zu diesem Zweck sind folgende Aspekte zu hinterfragen:

- Überprüfbare Referenzen
- Kompetenz und Verfügbarkeit des Ansprechpartners
- Vertrauenswürdigkeit der Mitarbeiter
- Zertifizierungen
- garantierte Verfügbarkeit (maximale Ausfallzeit) der Dienstleistungen
- Notfallplanung
- Sicherheitskonzept und Sicherheitsrichtlinien.

Für die Beurteilung muss bei größeren Auslagerungs-Vorhaben eine Besichtigung des Dienstleisters erfolgen.

4. Vertragsspezifische Regelungen

Dem Dienstleister darf generell erst dann Zugang zu IT-Systemen, Anwendungen und sicherheitsrelevanten Informationen gewährt werden, wenn eine Vertraulichkeitsvereinbarung unterzeichnet wurde.

Im Auslagerungs-Vertrag sind mindestens folgende Aspekte zu thematisieren:

- Einhaltung der einschlägigen Gesetze, Vorschriften und internen Regelungen
- Weisungsgebundenheit des Dienstleisters – Der Dienstleister hat die Weisungen des Auftraggebers hinsichtlich der bereitgestellten Dienste zu befolgen. Dies ist regelmäßig zu überprüfen. Ein Recht auf Prüfung ist vertraglich festzulegen.
- Stillschweigen über alle dem Dienstleister bekannt werdenden Informationen des Auftraggebers, welche nicht frei zugänglich sind.
- Benennung von Verantwortlichen/ Schnittstellen auf beiden Seiten:
 - Es ist sicherzustellen, dass diese ausreichende Befugnisse besitzen.
 - Spezielle Anforderungen an bestimmte Rollen können festgelegt werden. Es kann beispielsweise gefordert werden, dass ein Informationssicherheitsbeauftragter mit speziellen Kenntnissen (wie beispielsweise Host-Kenntnissen) beim Dienstleister benannt werden muss.
- Definition von Melde- und Kommunikationswegen
 - Alarmierungspläne (insbesondere dann, wenn Systeme an Standorten des Dienstleisters betrieben werden. In diesem Fall sind sofortige Alarmierungen des Auftraggebers bei unberechtigten Zutritts- oder Zugangsversuchen zu diesen Systemen sicherzustellen.)
 - Zeitrestriktionen für den Alarmierungsplan
- Zutritts-, Zugangs- und Zugriffsrechte für den Auftraggeber und für den Dienstleister – Diese müssen verbindlich festgelegt werden. In jedem Fall ist zu regeln, dass Entscheidungen über Zugangs- oder Zugriffsberechtigungen auf Informationen oder Systeme ausschließlich durch den Auftraggeber getroffen werden. Eine diesbezügliche Entscheidung durch Mitarbeiter des -Dienstleisters ist zu untersagen.
- Es ist zu regeln, welche Protokolldateien in welchem Umfang vom Dienstleister angelegt und ausgewertet werden müssen.
- Regelungen für den Fall der Nicht- oder mangelhaften Erfüllung
- Konkrete Sicherheitsanforderungen
 - Verfügbarkeitsanforderungen
 - Vertraulichkeitsanforderungen – Hierzu müssen alle Informationen hinsichtlich ihrer Vertraulichkeitsanforderung eingestuft werden.
 - Integritätsanforderungen
- Pflicht zur Ausarbeitung von IT-Sicherheitskonzepten. Dies beinhaltet insbesondere:
 - Technische und organisatorische Maßnahmen im Einflussbereich des Dienstleisters und dessen Kontrolle müssen festgelegt werden
 - Notfallvorsorge und -bewältigungsmaßnahmen sind zu planen und vertraglich festzulegen.
 - Alle Änderungen sind vorab auf Testsystemen zu testen.
 - Festlegungen zur Absicherung der Kommunikation zwischen dem Dienstleister und dem Auftraggeber bezüglich der zu verwendenden Verschlüsselungs- und Signaturverfahren.
 - Handelt es sich bei dem Auftragnehmer um einen Dienstleister, der dem Auftraggeber den Betrieb, Entwicklung oder Wartung einer individuellen Anwendung, Software oder Systemsoftware zur Verfügung stellt, ist folgendes vertraglich zu regeln:

- Der Dienstleister muss dem Auftraggeber die Lizenz zur Nutzung der Anwendung und relevanten Software zur Verfügung stellen.
- Der Dienstleister muss dem Auftraggeber eine aktuelle Dokumentation der Anwendung / Software sowie aktuelle operative Dokumentationen (Handbuch, Anleitungen zur Nutzung der Anwendung / Software) zur Verfügung stellen.
- Alle Informationen des Auftraggebers sind diesem durch den Dienstleister auf Verlangen des Auftraggebers vollständig, aktuell und in einem für Computer- und den Auftraggeber lesbaren Format innerhalb einer angemessenen Frist bereitzustellen.
- Bei Arbeiten des Dienstleisters beim Auftraggeber ist zusätzlich zu vereinbaren:
 - Externe Personen müssen sich ausweisen.
 - Sofern ein Zutritt zu Sicherheitszonen zwingend erforderlich ist, werden externe Mitarbeiter ständig beaufsichtigt. Kurzfristig oder einmalig zum Einsatz kommendes Fremdpersonal wird wie ein Besucher begleitet und beaufsichtigt.
- Regelungen zur Haftung
- Verfahren bei Beendigung des Vertrags
 - Zur Beendigung des Auftragsverhältnisses muss eine geregelte Übergabe der Arbeitsergebnisse und Betriebsmittel festgelegt werden.
 - Es ist außerdem zu vereinbaren, dass sämtliche eingerichteten Zugangsberechtigungen und Zugriffsrechte des Dienstleisters entzogen werden. Außerdem ist zu regeln, dass ausscheidende Mitarbeiter explizit darauf hingewiesen werden, dass die Verschwiegenheitsverpflichtung auch nach Beendigung der Tätigkeit bestehen bleibt.
 - Es ist zu regeln, dass Daten, die im Rahmen der Auslagerung extern gespeichert wurden, nach Abschluss des Auftrags vollständig und sicher zu löschen sind. Ein Kontrollrecht hierfür ist festzulegen.

5. Regelungen zum Notfallmanagement

Für die Notfallvorsorge und Notfallbewältigung bei der Auslagerung von Diensten gelten die gleichen Anforderungen wie beim nicht ausgelagerten Betrieb. Die Besonderheiten beim ausgelagerten Betrieb ergeben sich dadurch, dass auch das Notfallmanagement auf unterschiedliche Parteien aufgeteilt ist und durch die Verteilung der Komponenten auch zusätzliche Komponenten neu hinzukommen.

Generell müssen Notfallvorsorgekonzepte und Notfallpläne für die Systeme beim Auftraggeber, beim Dienstleister sowie für die Schnittstellen zwischen Auftraggeber und Dienstleister (wie Netzverbindung, Router, Telekommunikationsprovider) existieren und regelmäßig getestet sowie aktualisiert werden.

Zuständigkeiten, Ansprechpartner und Abläufe müssen klar geregelt und vollständig dokumentiert werden:

- Detaillierte Arbeitsanweisungen mit konkreten Anordnungen für bestimmte Fehlersituationen sind zu erstellen.
- Ein Konzept für Notfallübungen, die regelmäßig durchgeführt werden müssen, muss erarbeitet werden.

Die Informationssicherheit hängt in Notfällen entscheidend von der Qualität der Arbeitsanweisungen für das Personal des Dienstleisters ab. Oftmals werden die Systeme des Auftraggebers von Personal des Dienstleisters betrieben, das keine Detailkenntnisse über die Anwendungen besitzt, die auf den IT-Systemen betrieben werden. Die Verantwortung für die angemessene Sicherheit der Anwendung liegt dennoch ausschließlich beim Auftraggeber. Tritt ein Fehler in der Anwendung auf, muss der Dienstleister unter Umständen eine

Fehlerbehebung herbeiführen, ohne umfangreiche Kenntnisse über das System zu besitzen. Durch ein Notfallhandbuch müssen dem Dienstleister daher genaue Anweisungen zur Verfügung gestellt werden, wie er dabei vorgehen darf. Es kann dabei auch sinnvoll sein, Aktionen zu definieren, die explizit verboten sind (beispielsweise Reboot einer Maschine). Ein Fehlverhalten einer Anwendung kann technische Ursachen haben (beispielsweise Datenträger voll, Netzprobleme) oder anwendungsspezifische (beispielsweise Verarbeitung eines falschen Datensatzes, Programmfehler, falsche Parametereinstellung). Bei technischen Fehlern ohne Auswirkungen auf andere Anwendungen wird der Dienstleister den Fehler zwar selbst beheben können; meist ist aber dennoch eine Kooperation mit dem Auftraggeber notwendig, um ungewünschte Seiteneffekte auf Applikationsebene zu verhindern. Liegen anwendungsspezifische Probleme vor, benötigt der Dienstleister detaillierte und umfangreiche Anweisungen sowie Listen mit Ansprechpartnern auf Seiten des Auftraggebers, damit er richtig reagieren kann. Besonders bei Problemen mit komplexen Anwendungen oder bei umfangreichen Batch-Prozessen sind häufig Kenntnisse erforderlich, die nur beim Auftraggeber vorhanden sind.

Wichtig ist in diesem Fall auch, dem Dienstleister Informationen bezüglich des Schutzbedarfs der betroffenen Daten und Systeme zur Verfügung zu stellen, damit mit angemessener Umsicht gehandelt werden kann.

6. Inkrafttreten

Diese Richtlinie tritt als Informationssicherheitsrichtlinie mit sofortiger Wirkung in Kraft.

Augsburg, den 10.08.2021

gez.
Dr. Renate Linné
Stellv. Kaufmännische Direktorin

gez.
Markus Hoefer
Informationssicherheitsbeauftragter