Inhalt

1 Ziel und Geltungsbereich

Ziel dieser Richtlinie ist die Minimierung der für den Versorgungsauftrag entstehenden Risiken infolge von Dienstleistervereinbarungen sowie der Schutz der für Dienstleister und Lieferanten zugänglichen Assets und Informationen.

Es werden die aus Sicht der Informationssicherheit zu regelnden Aspekte aufgeführt, die in der Zusammenarbeit mit externen Dienstleistern zu beachten sind.

Das Klinikum Wolfsburg strebt damit auch die Einhaltung der Anforderungen aus Art. 25 und 32 der DSGVO an. Ein Abfallen des Sicherheitsniveaus durch Outsourcing bzw. die Neuschaffung von Produkten und Dienstleistungen muss vermieden werden.
Im Zusammenhang mit der Beschaffung von Produkten oder Dienstleistungen, mit Bezug zu Aspekten von Datenschutz oder Informationssicherheit, müssen die entsprechenden Vorgaben des Klinikums eingehalten werden.

2 Begriffsklärung

Dienstleister oder Lieferant im Sinne dieser Richtlinie sind alle externen Auftragnehmer des Klinikums, welche mindestens eines der folgenden Kriterien erfüllen:

- Dienstleister, die IT-Systeme, IT-Anwendungen, Netzwerkkomponenten, Infrastruktur-Komponenten, Medizingeräte oder Telekommunikationseinrichtungen aufstellen, warten, instandhalten, administrieren, konfigurieren oder reparieren
- Telekommunikations-Dienstleister
- Anbieter von Cloud-Diensten bzw. Managed Services
- Anbieter von im Internet frei verfügbaren Diensten wie Dropbox, WeTransfer, Virustotal
- Dienstleister, denen gezielt sicherheitsrelevante Daten bzw. Informationen des Klinikums übergeben werden, wie beispielsweise Sicherheitsdienstleister, Beratungsfirmen oder Wirtschaftsprüfer

3 Anforderungen

3.1 Managementaufgabe Informationssicherheit

Der Lieferant muss Rollen und Verantwortlichkeiten für die Informationssicherheit und gegebenenfalls den Datenschutz festlegen. Die personellen Ressourcen müssen ausreichend sein, um das geforderte Niveau des Datenschutzes und der Informationssicherheit realisieren zu können.
Auf Anfrage legt der Auftragnehmer Informationen seiner Sicherheitsorganisation offen, auf deren Basis das Klinikum eine Auftragnehmerbewertung durchführen kann.
Das Klinikum oder ein anderer beauftragter Dritter im Auftrag des Klinikums darf die Organisation des Auftragnehmers in Bezug auf die Informationssicherheit prüfen.

3.2 Schutz personenbezogener Daten

Sofern die Dienstleistung eine Verarbeitung personenbezogener Daten im Sinne von Art. 4 Nr. 2 EU-Datenschutzgrundverordnung (DSGVO) beinhalten kann oder die Kenntnisnahme personenbezogener Daten im Rahmen der Dienstleistungserbringung in sonstiger Weise nicht ausgeschlossen ist, sind die gesetzlichen und betrieblichen Datenschutzvorgaben durch den Dienstleister / Lieferanten einzuhalten.

3.3 Schulung und Sensibilisierung

Der Dienstleister muss sicherstellen, dass alle Mitarbeitende sowie ggf. Subunternehmer, die im Zusammenhang mit der gelieferten Dienstleistung bzw. des gelieferten Produktes Zugriff auf Informationswerte des Auftraggebers erhalten können, in angemessenem Umfang zur Informationssicherheit und gegebenenfalls zum Datenschutz geschult und sensibilisiert worden sind. Der Nachweis über die Schulung bzw. Sensibilisierung seiner Mitarbeitenden muss vom Dienstleister auf Nachfrage erbracht werden können.

3.4 Projektmanagement

Falls im Zusammenhang mit der gelieferten Dienstleistung bzw. dem Produkt auf der Seite des Dienstleisters Projektmanagement erforderlich ist, so muss im Projektmanagement die Informationssicherheit berücksichtigt werden. Insbesondere muss sichergestellt sein, dass im Rahmen der Projektkonzeption und bei der Projektabnahme das erforderliche Niveau der Informationssicherheit und gegebenenfalls des Datenschutzes realisiert wird.

3.5 Zulässiger Gebrauch von Werten

Der Dienstleister muss sicherstellen, dass die Regeln des Auftraggebers für den zulässigen Gebrauch von Informationen und Werten des Auftraggebers angewendet werden. Der Dienstleister kann ergänzend zu den Regeln des Auftraggebers eigene Regeln für den zulässigen Gebrauch von Informationen und Werten des Auftraggebers aufstellen. Dabei muss sichergestellt sein, dass die Regeln auf der Seite des Dienstleisters mindestens das Sicherheitsniveau des Auftraggebers erreichen.
Die Rückgabe von Werten des Auftraggebers bei Änderung oder Beendigung des Dienstleistungsverhältnisses wird ggf. im Hauptvertrag geregelt.

3.6 Informationsklassifizierung

Dem Dienstleiter wird die Dienstanweisung zur Klassifizierung von Informationen zur Verfügung gestellt. Er muss sicherstellen, dass die Regelung zur Kennzeichnung und zum Umgang mit klassifiziertem Material des Auftraggebers entsprechend dieser Richtlinie umgesetzt wird.

3.7 Zugangssteuerung

Falls der Dienstleister im Rahmen seiner Aufgaben z. B. für Support-Tätigkeiten auf Systeme des Auftraggebers zugreifen muss, so wird ihm hierfür ein Remotezugang eingerichtet. Der Dienstleister muss seinerseits sicherstellen, dass die Zugangsberechtigungen nur den Mitarbeitenden zugänglich sind, die die Supporttätigkeiten ausführen. Beim Ausscheiden dieser Mitarbeitenden ist das Klinikum Wolfsburg unverzüglich zu informieren, damit zugewiesene Berechtigungen entzogen werden können.
Für den Fall, dass für die Supporttätigkeit eigene Systeme des Lieferanten verwendet werden, muss dieser eine Zugangssteuerungsrichtlinie erstellen und umsetzen, sodass sichergestellt

wird, dass die betreffenden Systeme ausschließlich von den dazu berechtigten Mitarbeitenden verwendet werden.
Der Auftragnehmer muss sicherstellen, dass bei Fernzugängen die Vertraulichkeit, Verfügbarkeit ebenso wie die Integrität der Assets und Services des Klinikums gewährleistet sind.

3.8 Kryptografische Maßnahmen

Sollten im Zusammenhang mit der Dienstleitung kryptographische Maßnahmen erforderlich sein, so muss der Auftragnehmer sicherstellen, dass die geforderten Maßnahmen des Auftraggebers stets eingehalten werden. Dies gilt auch bei der verschlüsselten Kommunikation von Systemen bei Fernwartungstätigkeiten des Dienstleisters. Weiterhin ist dem Auftraggeber auf Wunsch eine Richtlinie zum Gebrauch der kryptographischen Schlüssel vorzulegen aus der hervorgeht, wie der Schutz sowie die Lebensdauer der Schlüssel beim Dienstleister geregelt sind.

3.9 Maßnahmen gegen Schadsoftware

Der Auftragnehmer muss sicherstellen, dass auf allen Computersystemen, die mittelbar oder unmittelbar im Zusammenhang mit der Dienstleistungserbringung verwendet werden, in angemessenem Umfang Maßnahmen zur Abwehr von Schadcode getroffen werden. Softwareprodukte zur Abwehr von Schadcode und Schadecode-Definitionen sind ständig aktuell zu halten. Davon betroffen sind insbesondere solche Geräte, die für Supporttätigkeiten für oder beim Auftraggeber Verwendung finden.

3.10 Protokollierung

Sofern im Zusammenhang mit der Dienstleistungserbringung von Seiten des Auftragnehmers Computersysteme zum Einsatz kommen, so hat der Auftragnehmer sicherzustellen, dass Ereignisse in angemessenem Umfang protokolliert werden. Der Zugriff auf die Protokollinformationen darf nur berechtigten Mitarbeitenden des Auftragnehmers oder des Auftraggebers erlaubt sein. Dies gilt insbesondere, falls im Rahmen der Protokollierung personenbezogene Daten gespeichert werden.
Die Protokollierung muss sicherstellen, dass Fehlersituation analysiert werden können. Die Protokollinformationen müssen im Fehlerfall oder bei Datenschutzverletzungen dem Auftraggeber unverzüglich auf Anfrage vorgelegt werden.

3.11 Umgang mit Sicherheitsvorfällen

Der Auftragnehmer ist verpflichtet, Sicherheitsvorfälle in seiner Organisation, die potenziell einen negativen Effekt auf die Systeme oder Daten des Klinikums haben könnten, unverzüglich dem Klinikum zu melden. Dies könnten z. B. auch Industriespionage, eine Softwareschwachstelle oder eine Sicherheitslücke in einer Systemkonfiguration sein.
Der Auftragnehmer unterstützt den Auftraggeber bei der Beurteilung von Sicherheitsvorfällen, die im Zusammenhang mit der beauftragten Dienstleistung stehen, indem er dem Auftraggeber alle relevanten Informationen im Zusammenhang mit dem jeweiligen Sicherheitsvorfall zur Verfügung stellt. Der Auftragnehmer legt Verfahren für die Ermittlung, Sammlung, Erfassung und Aufbewahrung von Informationen fest, die als Beweismaterial dienen können.

3.12 Informationsübertragung

Für einen betrieblichen Datenaustausch sind geeignete Maßnahmen zur Wahrung von Vertraulichkeit, Verfügbarkeit und Integrität zu vereinbaren.
Der Austausch von Daten muss auf geeigneten Plattformen erfolgen oder mit Mitteln die den Ansprüchen an die Einhaltung der Schutzziele der Informationssicherheit gerecht werden.
Eine Weitergabe der bereitgestellten Daten, Dokumente und Verfahren an Dritte ist nicht erlaubt.
Das Klinikum kann dazu ggf. formale Übertragungsrichtlinien, Verfahren und Maßnahmen vorgegeben.

3.13 Lieferantenbeziehungen

Falls der Auftragnehmer für die Erbringung der Dienstleistung Unterauftragnehmer in Anspruch nimmt, so hat der Auftragnehmer sicherzustellen, dass durch die Unterbeauftragung das geforderte Sicherheitsniveau nicht reduziert wird.

3.14 Compliance

Der Auftragnehmer hat sicherzustellen, dass angemessene Verfahren umgesetzt werden, um die Einhaltung gesetzlicher, regulatorischer und vertraglicher Anforderung mit Bezug auf geistige Eigentumsrechte und der Verwendung von urheberrechtlich geschützten Softwareprodukten zu gewährleisten.
Aufzeichnungen, die im Zusammenhang mit der beauftragten Dienstleistung stehen, müssen vom Auftragnehmer vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter Veröffentlichung geschützt werden.
Für den Fall, dass sich die Dienstleistung auf die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten bezieht, sind die entsprechenden Vorschriften des Datenschutzes von Seiten des Dienstleisters einzuhalten. Einzelheiten dazu werden im Vertrag zur Auftragsverarbeitung festgelegt.
Der Dienstleister sichert die Mitwirkung in geeigneter Weise bei der Pflege des Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 DSGVO zu.

3.15 Personaleinsatz

Nutzt externes Personal IT-Infrastruktur des Klinikums und/oder erhält einen internen E-Mail-Account und /oder Internet-Zugang, gelten die entsprechenden Regelungen des Klinikums.

3.16 Beendigung der Dienstleistung

Alle Daten, Dokumente und Informationen mit besonderem Schutzbedarf müssen nach Beendigung der Zusammenarbeit vom Dienstleister, gelöscht, zurückgegeben oder vernichtet werden. Dies gilt insbesondere für Informationen, welche die Informationssicherheit und Sicherheitsstrukturen des Auftraggebers betreffen. Entsprechende Nachweise über die Rückgabe, Löschung oder Vernichtung müssen durch die Dienstleister an das Klinikum Wolfsburg übergeben werden.

3.17 Patchmanagement

Bei einer Systemabnahme hat der Auftragnehmer sicherzustellen, dass alle Systeme vor der Abnahme nachweislich gepatcht und aktualisiert werden. Das Patch-Level sollte am Tag der Systemabnahmeerklärung immer aktuell sein. Der Auftragnehmer muss alle öffentlich verfügbaren und durch den Auftraggeber freigegebenen Patches als Teil der Lieferung installieren.

Soweit vertraglich nicht anders geregelt verpflichtet sich der Auftragnehmer, mindestens zweimal pro Jahr oder bei Bedarf unverzüglich Updates und Patches bereitzustellen, um die Anforderung aus dem Stand der Technik einzuhalten.

4 Inkrafttreten und Veröffentlichung

Diese Richtlinie tritt zum 30.04.2024 in Kraft und löst die Richtlinie vom 13.06.2023 ab
Die Veröffentlichung erfolgt im SharePoint unter Allgemein Klinikum.

Wolfsburg, den

Klinikum Wolfsburg
André Koch
Klinikumsdirektor

8. Mitgeltende Unterlagen

- Dienstanweisung zu Klassifizierung von Informationen

9. Dokumentenhistorie

Datum	Version	Autor	Bemerkung/ Änderung
30.11.2022	001	R. Gruetz	Freigabe
02.05.2023	002	R. Gruetz	Anpassung Logo
13.06.2023	002	A. Koch	Freigabe
25.03.24	003	R. Gruetz	Einfügen Patchmanagement
18.08.24	003	R. Gruetz	Einfügen Schutz personenbezogener Daten
30.04.24	003	A. Koch	Freigabe