Sicherheitsrichtlinie für Dienstleister und Lieferanten

Konzern-Richtlinie zu Datenschutz und Informationssicherheit

Christoph Schäfer | Datenschutzbeauftragter
Ralf Iffert | Informationssicherheitsbeauftragter
OA2203-02 | Version: 1.1 | Inkraftsetzung: 01.05.2025

Inhaltsübersicht

1. Ausgangslage 2
2. Umsetzung durch Lieferanten 2
3. Anforderungen an Lieferanten 3
3.1. Organisatorische Anforderungen an ein ISMS 3
3.1.1. Richtlinie zur Informationssicherheit beim Lieferanten 3
3.1.2. Rollen- und Verantwortlichkeiten 3
3.1.3. Sensibilisierung, Schulung und Verpflichtung 3
3.2. Technische und organisatorische Maßnahmen (TOMs) 3
3.2.1. Physische und umgebungsbezogene Sicherheit 3
3.2.2. Zugangssteuerung 3
3.2.3. Überprüfung von Benutzerzugangsrechten 4
3.2.4. Dokumentierte Bedienabläufe 4
3.2.5. Einsatz von Mobilgeräten und Telearbeit 4
3.2.6. Kryptographische Maßnahmen 4
3.2.7. Netzwerksicherheitsmanagement 5
3.2.8. Sicherung von Anwendungsdiensten in öffentlichen Netzwerken 5
3.2.9. Maßnahmen gegen Schadsoftware 5
3.2.10. Installation von Software auf Systemen 5
3.2.11. Einrichtung und Installation von netzwerkfähigen Komponenten 5
3.2.12. Umgang mit technischen Schwachstellen 5
3.2.13. Ereignisprotokollierung und Schutz der Protokollinformationen 6
3.2.14. Geschäftsfortführung im Notfall 6
3.2.15. Sicherung in Entwicklungsprozessen und Umgang mit Testdaten 6
3.2.16. Mindestumfang vertraglicher Regelungen 6
3.2.17. Lieferantenbeziehungen 7
4. Umgang mit Informationssicherheitsvorfällen 7
5. Maßnahmen zur Compliance 7

1. Ausgangslage

Die Gesundheit Nordhessen Holding AG und die mit ihr verbundenen Unternehmen mit einer Beteiligung von mehr als 50 % (im Folgenden: GNH) ist Betreiber Kritischer Infrastrukturen im Sinne der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV). Aus diesem Grund ergreift die GNH für alle technischen und nicht technischen Systeme Maßnahmen zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Belastbarkeit und Patientensicherheit. Dazu betreibt die GNH ein Informationssicherheitsmanagementsystem (ISMS) auf Basis des Branchenspezifischen Sicherheitsstandards (B3S) für die Patientenversorgung und hat einen Informationssicherheitsbeauftragten (ISB) bestellt, der Ansprechpartner für alle Fragestellungen im Zusammenhang mit der Informationssicherheit ist.

Der Zweck dieser Richtlinie ist es, Regeln für Lieferanten und Dienstleister (im Folgenden kurz: Lieferanten) zu definieren, damit die erforderliche Informationssicherheit auch bei beschafften Produkten und Dienstleistungen eingehalten wird. Umfasst sind dabei die Beschaffungen von Waren, Betriebs-/Hilfs-/Arbeitsmitteln, Hardware und Software mit Bezug zu Informationstechnik, Medizintechnik, Kommunikationstechnik und Versorgungstechnik (im Folgenden: Produkte) sowie die Erbringung von Dienstleistungen mit Bezug zu Informationssicherheit und Datenschutz. Umfasst sind alle schutzbedürftigen Unternehmenswerte, Prozesse oder Informationen, insbesondere personenbezogene Daten von Beschäftigten und Patient*innen der GNH (im Folgenden: Informationswerte). Diese Informationen können in physischer Form (z. B. Dokumente, Akten) und/oder digitaler Form (z. B. als Datei oder in Datenbanken) vorliegen. Die Anforderungen an die Informationssicherheit schließen diejenigen des Datenschutzes im Sinne der Datenschutz-Grundverordnung (DSGVO) und nachgelagerter Gesetze mit ein. Gleiches gilt in Bezug auf das Berufsgeheimnis im Sinne von § 203 Abs. 1 StGB bei der Verarbeitung von Patientendaten.

Der Informationssicherheitsbeauftragte (ISB) und der Datenschutzbeauftragte (DSB) werden frühzeitig in alle vorgenannten Beschaffungsprozesse eingebunden, um die Berücksichtigung der Anforderungen von Informationssicherheit und Datenschutz zu gewährleisten.

Die Anforderungen dieser Richtlinie müssen von allen Lieferanten der GNH umgesetzt werden, da sich durch die Beschaffung von Produkten oder Dienstleistungen das Niveau der Informationssicherheit nicht verschlechtern darf. Gleiches gilt auch beim Outsourcing. Die von Lieferanten getroffenen technischen und organisatorischen Maßnahmen zur Sicherstellung der Informationssicherheit müssen mindestens das Niveau der technischen und organisatorischen Maßnahmen der GNH erreichen.

2. Umsetzung durch Lieferanten

Da schützenswerte Informationswerte in nahezu allen Branchen und Bereichen zu finden sind und im Rahmen der Digitalisierung zunehmend an Bedeutung gewinnen und damit informationssicherheitstechnische Relevanz haben können, empfiehlt die GNH ihren Lieferanten von Produkten und Dienstleistungen, ein ISMS einzusetzen. Dabei können anerkannte Standards (beispielsweise B3S, ISO/IEC 27001, DIN EN 80001 oder BSI-Grundschutz) als normative Grundlagen dienen. Entsprechende Managementsysteme sind für Lieferanten für Produkte und Dienstleistungen in diesen Kategorien jedoch verbindlich, sofern sie im Rahmen von Ausschreibungen oder Verträgen explizit gefordert sind. Sofern Lieferanten ein solches Managementsystems einsetzen, muss der Geltungsbereich die gelieferten Produkte oder erbrachten Dienstleistungen vollständig einschließen.

Falls von Lieferanten kein geeignetes Managementsystem eingesetzt ist oder der Geltungsbereich des Managementsystems die gelieferten Produkte und Dienstleistungen nicht miteinschließt, so ist auf andere geeignete Weise die Einhaltung der Anforderungen dieser Richtlinie nachzuweisen.

Dabei müssen jedoch nur die Anforderungen erfüllt werden, die für das gelieferte Produkt bzw. die erbrachte Dienstleistung relevant sind. Anforderungen in Vergabeverfahren bzw. Verträgen gelten unabhängig von den Anforderungen dieser Richtlinie.

3. Anforderungen an Lieferanten

3.1. Organisatorische Anforderungen an ein ISMS

3.1.1. Richtlinie zur Informationssicherheit beim Lieferanten

Zentrale Regelungsdokumente der GNH sind die unternehmensbezogene *Leitlinie zur Informationssicherheit* und das *Rahmenkonzept Informationssicherheit und Datenschutz*. Das darin festgelegte Schutzniveau ist grundsätzlich auch von den Lieferanten zu gewährleisten. Falls auf der Seite des Lieferanten eine eigene Leitlinie zur Informationssicherheit – oder ein vergleichbares Dokument – vorhanden ist und diese die gelieferten Produkte oder erbrachten Dienstleistungen im Hinblick auf den Geltungsbereich des zugehörigen Managementsystems mit abdeckt, so müssen die Vorgaben des Lieferanten zu Datenschutz und Informationssicherheit mit den vorgenannten GNH-Dokumenten und dieser hier vorliegenden Richtlinie im Einklang stehen. Die Dokumente werden Lieferanten auf Nachfrage zur Verfügung gestellt.

3.1.2. Rollen- und Verantwortlichkeiten

Der Lieferant muss Rollen und Verantwortlichkeiten für die Informationssicherheit festlegen und ausreichend personelle Ressourcen vorhalten, um ein angemessenes Niveau an Informationssicherheit zu gewährleisten.

3.1.3. Sensibilisierung, Schulung und Verpflichtung

Der Lieferant muss sicherstellen, dass alle Beschäftigten, die im Zusammenhang mit den gelieferten Produkten oder den erbrachten Dienstleistungen Zugriff auf Informationswerte der GNH erhalten können, in angemessenem Umfang zur Informationssicherheit geschult und sensibilisiert worden sind. Der Nachweis über die Schulung bzw. Sensibilisierung seiner Beschäftigten muss vom Lieferanten auf Nachfrage erbracht werden können. Alle diese Beschäftigten müssen auf die Einhaltung der Informationssicherheit, des Datenschutzes und gegebenenfalls des Berufsgeheimnisses verpflichtet sein. Auf Verlangen der GNH können diese Beschäftigten zur Teilnahme an Sensibilisierungsmaßnahmen der GNH zu Datenschutz und Informationssicherheit verpflichtet werden.

3.2. Technische und organisatorische Maßnahmen (TOMs)

3.2.1. Physische und umgebungsbezogene Sicherheit

Der Lieferant muss durch geeignete Maßnahmen sicherstellen, dass der unbefugte Zutritt in Räume, Büros und Einrichtungen, in denen Informationswerte der GNH verarbeitet werden, ausgeschlossen ist. Dies gilt weiterhin auch für Anlieferungs- und Ladebereiche, über die unbefugte Personen die Räumlichkeiten betreten könnten. Besondere Bedeutung haben auch Büroräume, in denen Supporttätigkeiten über Remoteverbindungen durchgeführt werden. Im Idealfall regelt der Lieferant dies über eigene unternehmensbezogene Richtlinien.

3.2.2. Zugangssteuerung

Falls der Lieferant im Rahmen seiner Aufgaben, beispielsweise für Support-Tätigkeiten, auf Systeme der GNH zugreifen muss, so wird ihm hierfür ein Remotezugang eingerichtet oder ein Zugriff vor Ort gewährt. Der Dienstleister muss seinerseits sicherstellen, dass die Zugangsberechtigungen nur denjenigen Beschäftigten zugänglich sind, die die Supporttätigkeiten ausführen. Beim

Ausscheiden dieser Beschäftigten ist die GNH unverzüglich zu informieren, um die Zugangsberechtigungen zu entziehen und neue Zugangsberechtigungen vergeben zu können. Wenn für den Zugang ein Token erforderlich ist, muss dieses unter Verschluss gehalten bzw. vor dem Zugriff Dritter geschützt werden.

Der Zugriff des Lieferanten auf Systeme der GNH, darf ausschließlich über die von der GNH vorgegebenen Wege und autorisierten Zugänge erfolgen. Hierfür bestehen mehrere Gründe:

- Alle Fernwartungszugriffe werden nachvollziehbar protokolliert.
- Die Fernzugriffe sind auf das notwendige Maß beschränkt und werden nach vollzogenem Fernzugriff getrennt.
- Die GNH verringert durch die Verwendung eines einheitlichen Fernzugriffssystems ihre Cyber-Angriffsfläche.

Falls der Zugang über zwei Faktoren unter Verwendung eines Zugangstoken autorisiert wird, so muss der Dienstleister sicherstellen, dass der Zugriff auf das Token ausschließlich von dazu autorisierten Mitarbeitern ausgeübt werden kann. Erfolgen Fernzugriffe – beispielsweise aus technischen Gründen – nicht über den von der GNH favorisierten Weg, bedarf dies der Zustimmung der GNH und einer entsprechenden vertraglichen Regelung.

3.2.3. Überprüfung von Benutzerzugangsrechten

Sofern die Zugangsrechte der GNH von mehreren Beschäftigten des Lieferanten für den Zugang auf die Systeme der GNH genutzt werden, muss der Lieferant in regelmäßigen Abständen die Berechtigung zur Ausübung des Zugangs seiner Beschäftigten prüfen. Die Überprüfung der Berechtigungen ist zu dokumentieren und der GNH auf Nachfrage vorzulegen.

3.2.4. Dokumentierte Bedienabläufe

Der Lieferant ist angehalten, Bedienabläufe, die im Zusammenhang mit dem gelieferten Produkt oder der zu erbringenden Dienstleistung stehen, in angemessenem Umfang zu dokumentieren und dem Auftraggeber diese Dokumentation auf Anfrage vorzulegen.

3.2.5. Einsatz von Mobilgeräten und Telearbeit

Sofern im Zusammenhang mit den gelieferten Produkten oder erbrachten Dienstleistungen Zugriff auf Informationswerte oder Systeme der GNH erfolgt, so muss sichergestellt sein, dass dieser Zugriff ausschließlich innerhalb gesicherter Räume erfolgt. Ein Zugriff auf Informationswerte oder Systeme des Auftraggebers unter Verwendung von mobilen Endgeräten aus öffentlichen Bereichen heraus ist generell nicht erlaubt.

Diese Vorgabe gilt analog auch für den Fall, dass auf den Systemen des Lieferanten Informationswerte bzw. personenbezogene Daten der GNH verarbeitet werden.

Für den Fall, dass Informationswerte der GNH auf mobilen Speichermedien oder Festplatten in Laptops gespeichert werden, so müssen die Speichermedien bzw. Festplatten dem Stand der Technik entsprechend verschlüsselt sein.

3.2.6. Kryptographische Maßnahmen

Sollten im Zusammenhang mit dem gelieferten Produkt oder erbrachten Dienstleistung kryptographische Maßnahmen erforderlich sein, so muss die GNH sicherstellen, dass die geforderten Maßnahmen der GNH stets eingehalten werden. Dies gilt insbesondere bei der verschlüsselten Kommunikation von Systemen bei Fernwartungstätigkeiten des Lieferanten. Weiterhin ist der GNH auf

Wunsch eine Richtlinie zum Gebrauch der kryptographischen Schlüssel vorzulegen aus der hervorgeht, wie der Schutz sowie die Lebensdauer der Schlüssel beim Lieferanten geregelt sind.

3.2.7. Netzwerksicherheitsmanagement

Für im Rahmen des gelieferten Produkts oder der erbrachten Dienstleistung seitens des Lieferanten eingesetzte vernetzte Systeme, muss der Lieferant eigenverantwortlich sicherstellen, dass diese Netzwerke in angemessenem Umfang verwaltet und gesteuert werden, um sie vor Angriffen oder Störungen zu schützen. Dies kann insbesondere durch die gruppenweise Trennung von Informationsdiensten, Benutzern und Informationssystemen in Netzwerken umgesetzt werden (Netzwerksegmentierung).

3.2.8. Sicherung von Anwendungsdiensten in öffentlichen Netzwerken

Sofern von Seiten des Lieferanten im Zusammenhang mit der Dienstleistungserbringung Anwendungsdienste über öffentliche Netzwerke bereitgestellt werden, so hat er sicherzustellen, dass die Dienste vor betrügerischer Tätigkeit (insbesondere Hacker-Angriffen) und unbefugter Offenlegung oder Veränderung in angemessenem Umfang geschützt sind. Dies kann insbesondere in Form der regelmäßigen Durchführung von Penetrationstests erfolgen.

3.2.9. Maßnahmen gegen Schadsoftware

Der Lieferant muss sicherstellen, dass auf allen seinen Geräten und Systemen, die mittelbar oder unmittelbar im Zusammenhang mit der Dienstleistungserbringung bei der GNH verwendet werden, in angemessenem Umfang und dem Stand der Technik entsprechende Maßnahmen zur Abwehr von Schadcode getroffen werden. Softwareprodukte zur Abwehr von Schadcode und Schadcode-Definitionen sind stets aktuell zu halten.

3.2.10. Installation von Software auf Systemen

Der Lieferant muss sicherstellen, dass Betriebsabläufe auf Seiten der GNH durch die Installation von Software nicht ungeplant gestört werden. Die Installation von Software auf Systemen der GNH ist im Einzelfall mit den zuständigen Beschäftigten der GNH abzustimmen.

3.2.11. Einrichtung und Installation von netzwerkfähigen Komponenten

Sofern die gelieferten Produkte/Dienstleistungen netzwerkfähige Informationstechnik, Medizintechnik, Kommunikationstechnik oder Versorgungstechnik beinhaltet, müssen neben den medizinischen Anforderungen auch die Aspekte der IT-Sicherheit und des Datenschutzes berücksichtigt werden. Dazu liefert der Lieferant die notwendigen technischen Informationen zur Sicherstellung der GNH-eigenen Asset-, Risiko- und Schwachstellenmanagementprozesse. Bei netzwerkfähigen Medizinprodukten stellt der Lieferant ferner die notwendigen Informationen für ein Risikomanagement nach DIN EN 80001 zur Verfügung.

3.2.12. Umgang mit technischen Schwachstellen

Sofern für die Erbringung der beauftragten Dienstleistung oder des gelieferten Produkts Systeme oder Geräte des Lieferanten eingesetzt werden, ist der Lieferant verpflichtet, diese Systeme und Geräte in angemessenem Umfang und regelmäßig auf Schwachstellen zu überprüfen. Eine entsprechende Richtlinie muss der GNH nach Anforderung vorgelegt werden können.

Penetrationstests werden empfohlen. Schwachstellen müssen vom Lieferanten unverzüglich beseitigt werden, sofern dies technisch möglich ist. Die Durchführung von Schwachstellenprüfungen und ggfs. durchgeführten Penetrationstests muss der GNH auf Anfrage nachgewiesen werden können.

3.2.13. Ereignisprotokollierung und Schutz der Protokollinformationen

Sofern für die Erbringung der beauftragten Dienstleistung oder des gelieferten Produkts Systeme oder Geräte des Lieferanten eingesetzt werden, muss der Lieferant sicherstellen, dass informationssicherheitsrelevante Ereignisse in angemessenem Umfang protokolliert werden. Der Zugriff auf die Protokollinformationen darf nur berechtigten Beschäftigten des Lieferanten oder der GNH erlaubt sein. Dies gilt insbesondere, falls im Rahmen der Protokollierung personenbezogene Daten gespeichert werden. Die Protokollierung muss sicherstellen, dass Fehlersituationen analysiert werden können. Die Protokollinformationen müssen der GNH im Fehlerfall oder bei Datenschutzverletzungen vorgelegt werden.

3.2.14. Geschäftsfortführung im Notfall

Der Lieferant definiert Anforderungen an die Informationssicherheit und die Geschäftsfortführung in Abhängigkeit zur erforderlichen Verfügbarkeit des gelieferten Produkts oder der beauftragten Dienstleistung. Es ist sicherzustellen, dass die Dienstleistung gegen widrige Situationen (Krise oder Katastrophe) in angemessenem Umfang abgesichert ist. Der Verfügbarkeitsbedarf des gelieferten Produkts oder der beauftragten Dienstleistung ist mit der GNH abzustimmen. Der Lieferant legt Prozesse, Verfahren und Maßnahmen fest, dokumentiert diese und setzt sie um, damit das erforderliche Niveau an Informationssicherheit auch in widrigen Situationen aufrechterhalten werden kann. Die Wirksamkeit der Maßnahmen muss durch den Lieferanten in regelmäßigen Abständen geprüft werden. Die Prüfungen müssen dokumentiert und die Ergebnisse der GNH auf Verlangen nachgewiesen werden.

3.2.15. Sicherung in Entwicklungsprozessen und Umgang mit Testdaten

Sofern die Entwicklung von Software oder Systemen Gegenstand der Dienstleistung oder des Produkts ist oder in unmittelbarem Zusammenhang mit der Dienstleistungserbringung steht, so hat der Lieferant in eigener Verantwortung Richtlinien für die sichere Entwicklung von Software bzw. Systemen festzulegen und innerhalb seiner Organisation umzusetzen. Die Sicherheit von Entwicklungsumgebungen ist von Seiten des Lieferanten zu gewährleisten.

Wird die Entwicklung von Software oder Systemen im erlaubten Umfang vom Auftragnehmer an Unterauftragnehmer ausgelagert, so ist der Auftragnehmer verpflichtet, die Entwicklung in angemessenen Umfang zu überwachen. Während der Entwicklung müssen Sicherheitsfunktionen in angemessenem Umfang getestet werden. Systemabnahmetests – insbesondere für neue Systeme – sind durchzuführen und zu dokumentieren. Falls im Zusammenhang mit der Entwicklung vertrauliche Testdaten zur Verfügung gestellt werden, so hat der Lieferant die Vertraulichkeit der Testdaten zu gewährleisten.

Der Lieferant muss für die Entwicklung und den Test von Softwaren oder Systemen sicherstellen, dass Entwicklungs-, Test- und Produktivumgebungen voneinander getrennt sind.

Für Tests dürfen keine Produktivdaten verwendet werden, wenn es sich um personenbezogene Daten handelt.

3.2.16. Mindestumfang vertraglicher Regelungen

Der Lieferant und die GNH treffen mindestens zu den folgenden Aspekten der Informationssicherheit eine vertragliche Vereinbarung, sofern sie für die Lieferung der Produkte oder Erbringung der vereinbarten Dienstleistung relevant sind:

- Maßnahmen zur Datensicherung von Informationswerten der GNH, die durch den Lieferanten verarbeitet werden,

- Art der Übertragung von Informationswerten und Schutz derselben bei der Übertragung,
- Transport und Entsorgung von Datenträgern,
- Rückgabe von Informationswerten der GNH bei Änderung oder Beendigung der Vertragsbeziehungen,
- Vereinbarungen zum Datenschutz bei der Verarbeitung personenbezogener Daten.

3.2.17. Lieferantenbeziehungen

Falls der Lieferant für die Erbringung der Dienstleistung Unterauftragnehmer in Anspruch nimmt, so hat der Lieferant sicherzustellen, dass durch die Unterbeauftragung das Sicherheitsniveau, das die GNH vom Lieferanten fordert, nicht reduziert wird. Dazu sollen vom Lieferanten Richtlinien verwendet werden, die der vorliegenden entsprechen sollen. Der Auftragnehmer hat sicherzustellen, dass die Dienstleistungserbringung von Lieferanten seinen Vorgaben entspricht. Im Falle der Verarbeitung personenbezogener Daten sind vertragliche Regelungen gemäß der Art. 26 und 28 DSGVO zu treffen.

4. Umgang mit Informationssicherheitsvorfällen

Der Lieferant muss sicherstellen, dass Verantwortlichkeiten und Verfahren festgelegt werden, um eine schnelle, effektive und geordnete Reaktion auf Informationssicherheitsvorfälle zu ermöglichen. Sicherheitsvorfälle, die die beauftragte Dienstleistung bzw. das gelieferte Produkt betreffen oder Auswirkungen auf die GNH haben können, sind der GNH unverzüglich (binnen 24 Stunden) mitzuteilen. Der Lieferant ist verpflichtet, der GNH Schwächen in der Informationssicherheit mitzuteilen, die sowohl ihn selbst als auch die GNH betreffen, um es der GNH zu ermöglichen, geeignete Gegenmaßnahmen ergreifen zu können. Der Lieferant unterstützt die GNH bei der Beurteilung von Sicherheitsvorfällen, die im Zusammenhang mit der beauftragten Dienstleistung/Produkt stehen, indem er der GNH unverzüglich alle relevanten Informationen im Zusammenhang mit dem jeweiligen Sicherheitsvorfall zur Verfügung stellt. Der Lieferant legt Verfahren für die Ermittlung, Sammlung, Erfassung und Aufbewahrung von Informationen fest, die für die Analyse und Bewertung des Informationssicherheitsvorfalls relevant sein können (Beweismaterial).

Im Falle einer Verletzung des Schutzes personenbezogener Daten sind die Vorgaben des Art. 33 DSGVO zu beachten. Der Lieferant meldet der GNH unverzüglich und möglichst binnen 24 Stunden, nachdem ihm die Verletzung bekannt wurde, die Art und den Umfang der Verletzung.

5. Maßnahmen zur Compliance

Der Lieferant 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 dem gelieferten Produkt oder der beauftragten Dienstleistung stehen, müssen vom Lieferanten gemäß gesetzlichen, regulatorischen, vertraglichen und geschäftlichen Anforderungen vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter Veröffentlichung geschützt werden.