

RL ISMS Informationssicherheitsrichtlinie Lieferanten

TLP WHITE: Unbegrenzt

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP WHITE ohne Einschränkungen frei weitergegeben werden.

1 Zweck und Geltungsbereich

Dieses Dokument definiert Regelungen zur Informationssicherheit für Lieferanten, Dienstleister und Partner (nachfolgend „Lieferanten“ genannt). Es fasst die Inhalte des Informationssicherheitsmanagementsystems (ISMS) zusammen, um den Lieferanten ein Grundverständnis für die Sicherheitsanforderungen und -verfahren im Ortenau Klinikum zu vermitteln. Es gilt für alle Lieferanten, welche im und für den Geltungsbereich des Informationssicherheitsmanagementsystems im Ortenau Klinikum tätig sind oder anderweitig schützenswerte Informationen (bspw. Betriebsgeheimnisse, Know-how oder sonstige vertrauliche Informationen) des Ortenau Klinikum verarbeiten.

2 Verantwortlichkeit

Der Vorstand des Ortenau Klinikum hat einen Informationssicherheitsbeauftragten ernannt, der für die Umsetzung und Überwachung des Informationssicherheitsmanagementprozesses im Ortenau Klinikum verantwortlich ist.

Der Lieferant ist für jene Belange der Informationssicherheit verantwortlich, welche seine Geschäftsbeziehung mit dem Ortenau Klinikum beeinflussen. Die Lieferanten des Ortenau Klinikum sind verpflichtet, sich entsprechend der Informationssicherheitsleitlinie des Ortenau Klinikum zu verhalten und die Anforderungen dieser Richtlinie sowie aller daraus abgeleiteten Anforderungen zu erfüllen.

3 Anforderungen an Lieferanten

1. Der Lieferant des Ortenau Klinikum verpflichtet sich, bei der Auftragsausführung alle einschlägigen Vorschriften, Normen, Verordnungen und Gesetze sowie die allgemein anerkannten Regeln der Technik einzuhalten und verpflichtet auch seine Subunternehmer sowie von diesen eingesetzte weitere Auftragnehmer entsprechend.
2. Der Lieferant ist zur Einhaltung der datenschutzrechtlichen Bestimmungen verpflichtet. Er hat seine Mitarbeiterinnen und Mitarbeiter sowie von ihm beauftragte Subunternehmer auf die Einhaltung der datenschutzrechtlichen Bestimmungen hinzuweisen und zu verpflichten. Im Falle der Verarbeitung personenbezogener Daten ist je nach Sachverhalt ein Vertrag zur Auftragsverarbeitung gem. Art. 28 DSGVO, bzw. ein Vertrag zur gemeinsamen Verantwortung gem. Art. 26 DSGVO ergänzend abzuschließen. Im Rahmen dieser Verträge sind auch gesonderte Vereinbarungen zur Einhaltung der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO zu treffen. Sofern Sozial- und/oder Gesundheitsdaten in einem Cloudsystem verarbeitet werden, hat die datenverarbeitende Stelle die Anforderungen des §393 SGB V zu erfüllen und auf Anfrage nachzuweisen.
3. Der Lieferant verpflichtet sich Betriebsgeheimnisse, Know-how und sonstige vertrauliche Informationen vertraulich zu behandeln. Eine Ausnahme besteht, wenn die vertraulichen Informationen bereits allgemein bekannt sind oder der Lieferant sie ohne Verletzung der Vertraulichkeitspflicht öffentlich macht. Der Lieferant hat zudem dafür Sorge zu tragen, dass auch seine Mitarbeitenden sowie von ihm beauftragte Subunternehmer zur Vertraulichkeit verpflichtet werden. Dies gilt auch für zufällig zur Kenntnis genommene Daten und sonstigen Informationen. Die Vertraulichkeitsverpflichtung erstreckt sich über die gesamte Dauer des Vertragsverhältnisses sowie die Zeit nach dessen Beendigung. Der § 203 StGB wird dabei explizit berücksichtigt. Das Ortenau Klinikum behält sich das Recht vor die Herausgabe seiner beim Lieferanten gespeicherten oder verarbeiteten Informationen anzufordern.

RL ISMS Informationssicherheitsrichtlinie Lieferanten

4. Der Lieferant hat dafür Sorge zu tragen, dass die Mitarbeitenden und Subunternehmer, welche Informationen des Ortenau Klinikum verarbeiten, über die geltenden Anforderungen informiert sind und die Regelungen aus dieser Richtlinie einhalten.
5. Sofern ein Fernwartungszugang notwendig ist, sind ergänzende Regelungen zur Durchführung dieser Zugriffe zu vereinbaren.
6. Der Lieferant verpflichtet sich dazu, bei der Auftragsausführung ausschließlich fachlich geeignetes und ausreichend geschultes Personal einzusetzen.
7. Der Lieferant erkennt an, dass die eigenständige Nutzung oder Schaffung von Zutritts-, Zugangs- und Zugriffsberechtigungen zum Ortenau Klinikum untersagt ist, sofern sie nicht seitens des Ortenau Klinikum genehmigt wurden.
8. Geräte, Dokumente, Informationen usw. die dem Lieferanten vom Ortenau Klinikum zur Verfügung gestellt werden, bleiben Eigentum des Ortenau Klinikum.
9. Die Verwendung, Reproduktion oder Entfernung von Datenträgern, Akteninhalten oder sonstigen Informationen jedweder Art, die im Rahmen der Vertragsausführung zugänglich sind, ist ausschließlich mit Zustimmung des Ortenau Klinikum gestattet.
10. Schützenswerte Daten sind stets verschlüsselt zu übermitteln.
11. Um die Vertraulichkeit schutzbedürftiger Informationswerte sicherzustellen, müssen diese nach Gebrauch so vernichtet oder gelöscht werden, dass eine Rekonstruktion der Informationen mit hoher Wahrscheinlichkeit ausgeschlossen werden kann.
12. Der Lieferant hat angemessene organisatorische und technische Vorkehrungen zu treffen, um Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit seiner informationstechnischen Systeme, Komponenten oder Prozesse, die zur Erbringung seiner Dienstleistungen oder zur Nutzung seiner Produkte erforderlich sind, zu vermeiden. Dabei ist der Stand der Technik zu berücksichtigen.

3.1 Meldung von Informationssicherheitsvorfällen und Schwachstellen

Sobald bei dem Lieferanten ein Informationssicherheitsvorfall eintritt, der Auswirkungen auf an das Ortenau Klinikum gelieferte Produkte oder Dienstleistungen hat oder auf andere Weise die Informationssicherheit des Ortenau Klinikum gefährdet, ist das Ortenau Klinikum unverzüglich und ohne schuldhaftes Zögern vom Lieferanten zu informieren. Diese Informationspflicht gilt auch wenn Zweifel über die Auswirkungen auf das Ortenau Klinikum bestehen, Auswirkungen also nicht konkret ausgeschlossen werden können.

Informationssicherheitsvorfälle und Schwachstellen sind an folgende E-Mail-Adresse zu melden:

it-sicherheit[at]ortenau-klinikum.de

Der Lieferant hat in diesem Zusammenhang auch einen Ansprechpartner zu nennen, der bei Rückfragen kontaktiert werden kann.

4 Überprüfung

Der Lieferant räumt dem Ortenau Klinikum das Recht und die Möglichkeit ein, die relevanten Prozesse und Maßnahmen dieser Richtlinie zu auditieren. Der Lieferant erklärt sich bereit, die im Rahmen von Audits festgestellten Abweichungen in einer gemeinsam vereinbarten Frist zu beheben, es sei denn, dass die Behebung aus wirtschaftlichen, prozessualen oder sonstigen Gründen nicht vertretbar ist.

5 Mitgeltende Dokumente

LL ISMS Informationssicherheitsleitlinie

https://www.ortenau-klinikum.de/fileadmin/user_upload/PDFs/Verbund/LL_ISMS_Informationssicherheitsleitlinie_website.pdf