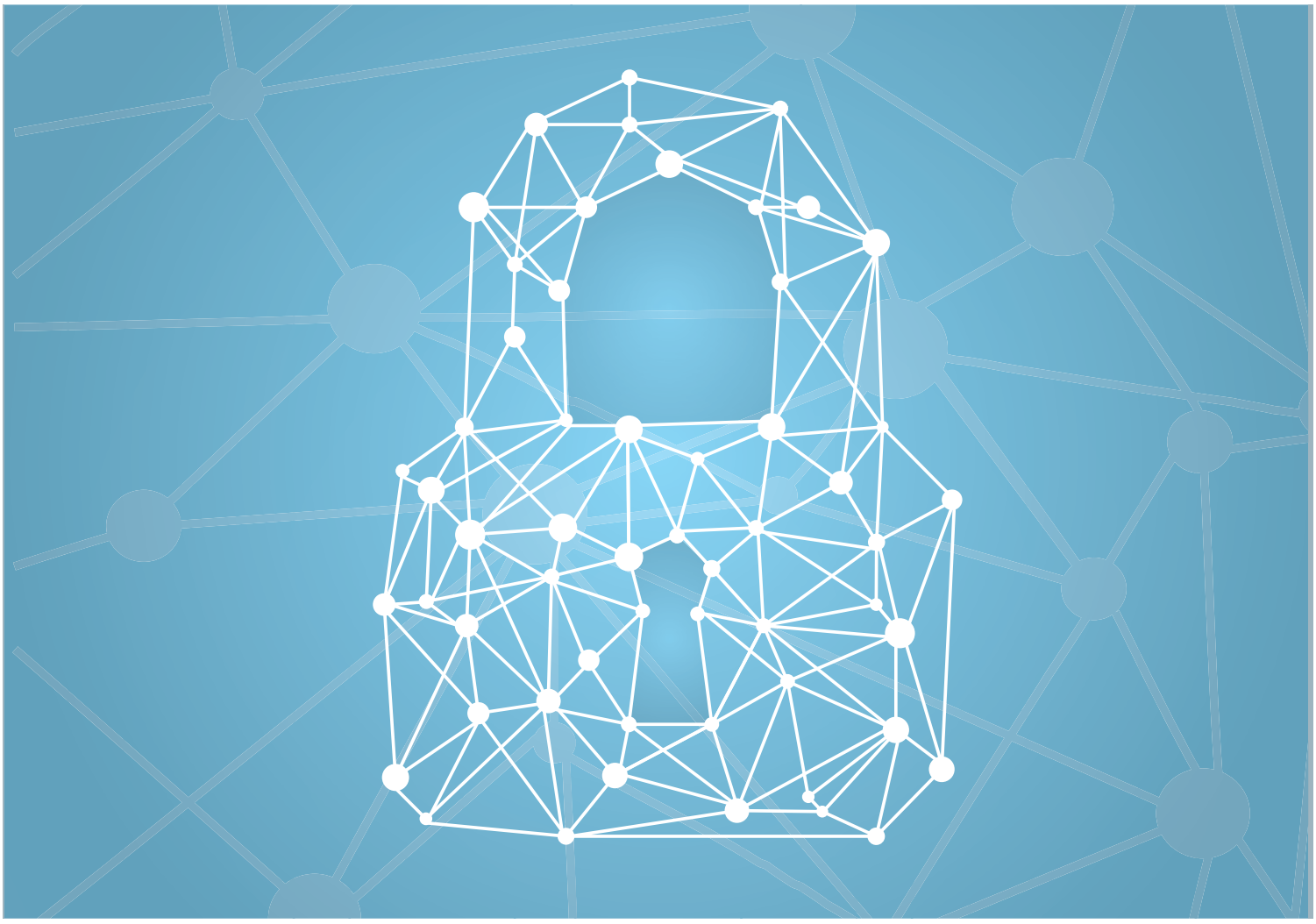
KAMP



VERSCHLÜSSELUNG VON DATEN-VERBINDUNGEN IM HEALTH-CARE-BEREICH

DIN ISO/IEC 27001 ZERTIFIZIERT

IT-SICHERHEIT 27002 GEPRÜFT

CLOUD-DIENSTE 27018 GEPRÜFT

DIN EN ISO 9001 ZERTIFIZIERT

DEUTSCHER RECHENZENTRUMSPREIS 2014

VERSCHLÜSSELUNG VON DATEN-VERBINDUNGEN IM HEALTH-CARE-BEREICH

In der Datenkommunikation im Health-Care-Bereich werden in der Regel personenbezogene Daten übertragen. Ob bei der Alarmierung von Rettungskräften über Pager oder der Datenkommunikation über die Anbindung der Einrichtung – häufig werden personenbezogene Gesundheitsdaten übermittelt, die nach aktueller Rechtslage als besonders schützenswert gelten. Daraus resultieren entsprechende Anforderungen an die IT-Infrastruktur im Gesundheitssektor, die sowohl Vertraulichkeit als auch Integrität durch kryptographische Verfahren gewährleisten soll.

Die seit dem 25. Mai 2018 geltende Datenschutz-Grundverordnung legt europaweit den Umgang mit personenbezogenen Daten fest. Alle Unternehmen und Organisationen sind zur Einhaltung der datenschutzrechtlichen Regelungen verpflichtet.

[1] Datenschutz-Grundverordnung (DSGVO)

Artikel 32 DSGVO besagt: „Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art des Umfangs der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten."

Nach Erwägungsgrund 75 ergeben sich bei der Verarbeitung von Gesundheitsdaten besondere „Risiken für die Rechte und Freiheiten natürlicher Personen."

Nach Artikel 4 Z. 15 DSGVO: sind unter „Gesundheitsdaten" diejenigen personenbezogenen Daten zu verstehen, „die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen."

Das BSI ist als obere Bundesbehörde für die Fragen der IT-Sicherheit zuständig. Mit dem BSI-Gesetz, das am 25.07.2015 in Kraft getreten ist, wurde der zunehmenden Bedeutung der Sicherheit in der Informations- und Kommunikationstechnologie Rechnung getragen.

[2] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)

§ 8a Abs. 1: Betreiber [...] sind verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen und Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse [...] zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen [...] Infrastrukturen maßgeblich sind."

Die Technische Richtlinie 03116-1, Abschnitt 2.1. des BSI besagt, dass bei der Übertragung von Gesundheitsdaten sowohl die „Vertraulichkeit" als auch die „Integrität" der Daten durch kryptographische Verfahren gewährleistet werden soll.

Für eine rechtskonforme Datenkommunikation im Health-Care-Bereich sollten folglich die Maßnahmen für den Schutz der personenbezogenen Gesundheitsdaten dem **Stand der Technik** entsprechen. Dabei muss der Vertraulichkeit und Integrität der übertragenen Daten Rechnung getragen werden. Dieses Sicherheitsniveau kann nur anhand einer Verschlüsselung erreicht werden.

KAMP Netzwerkdienste GmbH
Vestische Straße 89–91 | 46117 Oberhausen **Kontakt** Fon: +49 (0) 208.89 402-0 | Fax: +49 (0) 208.89 402-40 | Internet: www.kamp.de | E-Mail: info@kamp.de