Neue Entschließung der DSK für Krankenhäuser

Dortmund, 26. November 2019: Die Datenschutzkonferenz der Aufsichtsbehörden in Bund und Ländern (DSK) hat auf ihrer letzten Sitzung in Trier am 6./7.11.2019 (98. Datenschutzkonferenz) sich intensiv mit dem Datenschutz in Krankenhäusern befasst. Der Gesundheitsbereich bildete einen Schwerpunkt der Konferenz. Dabei wurden für Krankenhäuser eine neue Entschließung und eine Orientierungshilfe erarbeitet.

Gesundheitseinrichtungen müssen unabhängig von ihrer Größe den Schutz von Patientendaten gewährleisten
In dieser Entschließung wird noch einmal betont, dass Patientendaten im Rahmen der elektronischen Verarbeitung keineswegs sicher sind und auch nicht immer datenschutzkonform gespeichert werden. In jüngster Zeit sind dabei zwei wesentliche Bedrohungen aufgetreten:

1. Der Befall von Krankenhausinformationssystemen mit Schadsoftware, mit welcher Patientendaten verschlüsselt wurden, so dass sie für die Klinik nicht mehr zugänglich waren. Dies führte zu einer erheblichen Behinderung des Krankenhausbetriebs.
2. Die DSK wies daraufhin, dass im September dieses Jahres bekannt wurde, dass 16 Millionen Patientendatensätze – davon 13000 aus deutschen Gesundheitseinrichtungen – offen im Netz zugänglich waren. Als Ursache hierfür wurden unzureichende technische und-organisatorische Vorkehrungen benannt.

Die DSK hat deshalb dazu aufgefordert, dass auch in kleineren Einrichtungen die finanziellen Möglichkeiten geschaffen werden, dass die nach dem Stand der Technik gesetzlich gebotenen Vorkehrungen ergriffen werden können.

Link zur Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 06.11.2019

Orientierungshilfe für Messenger-Dienste im Krankenhausbereich
Die DSK hat am 7.11.2019 ein „Whitepaper zu technischen Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich“ als Orientierungshilfe veröffentlicht. Die Notwendigkeit solche Dienste auch im Gesundheitsbereich zu nutzen, wird auf Grund der Vielseitigkeit, Kostengünstigkeit und großer Verbreitung auch im persönlichen Bereich, nicht in Frage gestellt. Dabei müssen jedoch, gerade bei der Übermittlung medizinischer Daten die Anforderungen nach § 11 KDG (Art. 9 DSGVO) gewahrt bleiben. Die DSK führt hierzu folgendes aus:

„Der berufliche oder gewerbliche Einsatz von Messenger-Diensten unterliegt gesetzlichen Datenschutz-Vorgaben, denen gängige Messenger-Dienste bislang nicht oder nur bedingt entsprechen. Insbesondere der verbreitet genutzte Dienst WhatsApp führt bei einer geschäftliche Nutzung zu einer Reihe von Problemen, die einen Einsatz im Krankenhaus weitgehend ausschließen. Ähnliches gilt für andere im privaten Bereich häufig genutzte Dienste.“

Deshalb sind für die Auswahl von Messenger-Diensten im Krankenhaus die in dieser Orientierungshilfe genannten Datenschutzanforderungen zu berücksichtigen.

1. Hinsichtlich der eingesetzten Applikation werden 13 Punkte benannt. Sie umfassen unter anderem die Information der Nutzer, ihre Authentifizierung, die Sicherstellung der Verfügbarkeit der Daten, bis hin zur Konfiguration datenschutzgerechter Einstellungen und automatischer Update-Verfahren.
2. Zur Kommunikation sind 4 Stichworte genannt: Hierbei wird die vollständige Vertraulichkeit durch eine Ende-zu-Ende-Verschlüsselung gefordert, ebenso wie die Speicherung der Verbindungsdaten höchstens für den Zeitraum der Dauer der Verbindung. Meta-Daten dürfen nur vom Krankenhaus selbst aber nicht vom Provider genutzt werden. Ferner soll zumindest optional die Nutzung offener Kommunikationsprotokolle möglich sein.
3. Die Sicherheit der Endgeräte soll durch wirksamen Zugriffsschutz, regelmäßige Sicherheitspatches und Unterwerfung unter ein Mobile Device Management (3 Anforderungen) sichergestellt werden.
4. Schließlich werden Anforderungen an die Plattform / den ggf. externen Betrieb des Messenger-Dienstes in 9 Punkten geregelt. Diese umfassen einerseits die Beachtung der Vorschriften nach DSGVO und TKG bei öffentlich zugänglichen Diensten. Andererseits darf die Teilnahme am Dienst nur innerhalb einer geschlossenen Nutzergruppe bei entsprechender Autorisierung und Registrierung möglich sein. Für die Nutzung der mit dem

Messenger-Dienst verbundenen Verarbeitungstätigkeiten muss eine Datenschutz-Folgenabschätzung durchgeführt werden. Auftragsdatenverarbeiter können unter Beachtung der geltenden Regelungen einbezogen werden. Empfohlen werden Dienstleister aus Deutschland, der Europäischen Union bzw. dem europäischen Wirtschaftsraum. Schließlich ist eine regelmäßige Kontrolle durch das Krankenhaus als verantwortliche Stelle vorzunehmen. Idealerweise erlaubt die eingesetzte Messenger-Lösung auch einen Betrieb auf der Infrastruktur des Krankenhauses.

In diesem Zusammenhang sei auch noch einmal auf den Beschluss der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche in Deutschland zur Beurteilung von Messenger- und anderen Social Media-Diensten hingewiesen. >> zum Beschluss >>