Selbstdatenschutz & digitale Selbstverteidigung

Datenschutz-Zertifizierung im Gesundheitswesen

- Heidelberger Datenschutz-Rating (HDR) -

9 Antworten von Mark Peters **Heidelberg, März 2018**

Bald tritt die DS-GVO europaweit in Kraft und ändert somit auch das Bundesdatenschutzgesetz (BDSG). Die neuen Regeln gelten ab Mai 2018. Dabei ist es von großem Vorteil über die neuen Verordnungen Bescheid zu wissen und so die Herausforderung zu meistern. Eine Zertifizierung im Datenschutz bedeutet, dass dieses Ziel erreicht ist und das Unternehmen sich einer Prüfung durch die Aufsichtsbehörde getrost stellen kann.

Was bedeutet es, wenn die Zertifizierung im Gesundheitswesen verliehen wird?

Wer eine Datenschutz-Zertifizierung gemäß dem Heidelberger Datenschutz-Rating erhält, hält sich an die Inhalte der DS-GVO und ist motiviert diese dauerhaft und mit vollem Einsatz von Herzen umzusetzen.

Was für Vorteile hat es ein Datenschutz-Zertifikat zu besitzen?

Durch die Heidelberger Datenschutz-Rating-Zertifizierung wird der Datenschutz für alle Beteiligten transparent. Das stärkt vor allem Vertrauen. So wissen die Patienten und Angehörigen, dass ihre Daten in sicheren Händen sind. Das Zertifikat führt außerdem zu einem positiven Öffentlichkeitsbild.

Was muss erfüllt werden, um eine Zertifizierung zu erhalten?

Es muss eine Umsetzung der DS-GVO zu sehen sein. Eine Sensibilisierung für das Thema Datenschutz und die Umsetzung im Tagesgeschäft vor allem im technischen und organisatorischen Geschehen muss vorliegen. Vor allem die technischen Maßnahmen werden immer wichtiger, da Arztpraxen immer öfter Opfer von Cyberangriffen werden und zum Wohle des Datenschutzes sich auf solche Attacken vorbereiten müssen. Insofern hängen Datenschutz und IT-Sicherheit in höchstem Maße miteinander zusammen.

Datenschutzprüfungen durch die Behörden

Das LDA führt im Rahmen seiner gesetzlichen Aufgaben regelmäßig anlassbezogene und anlasslose Datenschutzprüfungen vor Ort gemäß BDSG § 38 Abs. 1 Satz 1 durch.

Mit der HDR-Zertifizierungen weisen Sie die Einhaltung bzw. die kontinuierliche Weiterentwicklung der DS-GVO Grundlagen nach.

Wie lange gilt eine Zertifizierung?

Unser Heidelberger Hygiene Rating Zertifikat gilt maximal für 3 Jahre, wobei eine jährliche unangemeldete Prüfung durchgeführt werden kann, bei der inspiziert wird, ob die Voraussetzungen immer noch erfüllt werden. Es ist wichtig die Zertifizierung nicht über einen zu langen Zeitraum zu vergeben um zu gewährleisten, dass die Vorgaben weiterhin erfüllt werden.

Wie kann man sich am besten auf den Zertifizierungsprozess vorbereiten?

Durch gezielte Schulungen sollten sich sowohl die Geschäftsleitung als auch die Mitarbeiter (ins besondere die, die an der Datenverarbeitung beteiligt sind) mit dem Datenschutz bekannt machen. Es müssen Ist-Soll-Analysen durchgeführt werden und auf den Soll-Zustand hingearbeitet werden. Dies ist durch ein durchdachtes Datenschutzmanagementsystem, das bei Schulungen gelehrt wird, möglich. Die DS-GVO muss motiviert umgesetzt werden. Dabei sind die wichtigsten Punkte: einen Notfallplan entwickeln bei Verstößen gegen die Verordnung und eine adäquate Dokumentation der Datenverarbeitung (beispielsweise der Datenschutz-Folgenabschätzungen o. ä.).

Was für Voraussetzungen sollte ein externer Datenschutzbeauftragter im Gesundheitswesen erfüllen?

- 10 Jahre Erfahrung im Gesundheitswesen und der Organisation
- Erfahrung als QM Beauftragter und Auditor im Gesundheitswesen
- IT Erfahrung
- anerkannte Ausbildung zum Datenschutzbeauftragten
- ständige Weiterbildung
- gute Referenzen aus dem Gesundheitswesen

Mark Peters, Heidelberg IT & Datenschutzexperte, Auditor im Gesundheitswesen bei Praxismanagement Bublitz-Peters

Was für Prüfungen müssen bestanden werden, um das Zertifikat zu erlangen?

Es muss gezeigt werden, dass die wichtigsten Punkte der DS-GVO im Unternehmen automatisch eingehalten werden. Dazu gehören beispielsweise das Führen eines Verzeichnisses für Verarbeitungstätigkeiten oder der Nachweis, dass bei besonders sensiblen Verarbeitungsvorgängen eine Datenschutz-Folgenabschätzung durchgeführt wird.

Wie kann nach Ablauf der Zertifizierung diese erneuert werden?

Um die Voraussetzungen weiterhin zu erfüllen, braucht es einen kontinuierlichen Verbesserungsprozess. Dazu sollten Schulungen und Weiterbildungen zum Thema Datenschutz besucht werden. Sehr wichtig ist auch die stetige Dokumentation, anhand derer man die Fortschritte besonders gut erkennt.

Kann man trotz der Zertifizierung bei Fehlern noch belangt werden?

Ganz wichtig ist, dass trotz einer Zertifizierung stets die Verantwortung bestehen bleibt. Das Zertifikat entbindet nicht von der Pflicht sich weiterhin mit dem Thema zu beschäftigen und stets auf dem neusten Stand zu bleiben und den Datenschutz täglich umzusetzen. Vielmehr ist es ein Mittel der Selbstevaluierung, sich immer wieder damit auseinander zu setzen, ob die Zertifizierungsrichtlinien stets erfüllt werden.

Infos auf:
www.datenschutzzertifizierung.info

Ab dem 25. Mai 2018 gelten:
EU-Datenschutz-Grundverordnung (EU-DSGVO) das neue BDSG
EU-ePrivacy-Verordnung

Praxismanagement Bublitz-Peters GmbH & Co. KG, Rohrbacher Str. 28, 69115 Heidelberg, Telefon: 0 62 21- 43 85 00
Telefax: 0 62 21- 43 85 01 10 E-Mail: info@bublitz-peters.de www.bublitzpeters.de C-10.314