Technisches und rechtliches Rezertifizierungs-Gutachten - Kurzgutachten -

"RED Medical"

für:
RED Medical Systems GmbH
Josef-Jägerhuber-Straße 7
82319 Starnberg

für das Gütesiegel für IT-Produkte (ULD)

erstellt von:

Andreas Bethke
Dipl. Inf. (FH)
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (technisch)

Papenbergallee 34
25548 Kellinghusen
tel 04822 – 37 89 05
fax 04822 – 37 89 04
mob 0179 – 321 97 88
email bethke@datenschutz-guetesiegel.sh

Stephan Hansen-Oest
Rechtsanwalt
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (rechtlich)

Neustadt 56
24939 Flensburg
tel 0461 – 90 91 356
fax 0461 – 90 91 357
mob 0171 – 20 44 98 1
email sh@hansen-oest.com

Stand: 13.12.2016

A. Einleitung

Die RED Medical Systems GmbH strebt die Rezertifizierung ihres Produktes „RED Medical" für das Gütesiegel für IT-Produkte des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) an.

Die Vorlage eines rechtlichen und technischen Gutachtens ist Voraussetzung für die Rezertifizierung des Produktes. Dieses Dokument dient als Gutachten zur Vorlage beim ULD im Zusammenhang mit der Rezertifizierung des Produktes.

Dem Gutachten wird der Anforderungskatalog in der Version 2.0 zugrunde gelegt.

Eine Änderung an dem Produkt gab es seit der letzten Rezertifizierung am 19.12.2014 nicht.

B. Zeitpunkt der Prüfung

Die Prüfung des Produktes fand vom 01.11.2016 bis zum 20.11.2016 statt.

C. Änderungen und Neuerungen des Produktes

Seit der Rezertifizierung des Produktes im Dezember 2014 haben sich am Produkt selbst keine Produktänderungen ergeben. Jedoch wurde seit der letzten Rezertifizierung der Anforderungskatalog angepasst, so dass eine neue Bewertung erfolgen muss.

D. Datenschutzrechtliche Bewertung

Seit der letzten Rezertifizierung wurde der Anforderungskatalog des ULD Gütesiegels angepasst. Darum soll an dieser Stelle die neue tabellarische Darstellung erfolgen.

Anforderung nach Katalog oder sonstigen Rechtsnormen	**Bewertung**	**Kommentare**
Komplex 1:		
1.1 IT-Sicherheits-Schutzziele: Verfügbarkeit, Integrität, Vertraulichkeit	adäquat	Durch die browserbasierte Lösung bleibt das Restrisiko des Ausfalls der Internetanbindung, für den der Hersteller nicht verantwortlich ist.

Anforderung nach Katalog oder sonstigen Rechtsnormen	**Bewertung**	**Kommentare**
1.2 Datenschutz-Schutzziel: Nicht-Verkettbarkeit (inkl. Datensparsamkeit, Zweckbindung und Zwecktrennung)	adäquat	Es werden lediglich Daten erhoben, die zur Behandlung und Abrechnung von Patienten benötigt werden.
1.3 Datenschutz-Schutzziel: Transparenz (inkl. Produktbeschreibung)	adäquat	
1.4 Datenschutz-Schutzziel: Intervenierbarkeit	adäquat	Die Intervenierbarkeit ist durch die einsetzende Stelle gegeben.
1.5 Anpassung des IT-Produkts	adäquat	Das Produkt unterliegt den Anforderungen durch Gesetzgeber und Versicherungen, so dass eine permanente Anpassung obligatorisch ist.
1.6 Privacy by Default	adäquat	Das Produkt wird mit datenschutzfreundlichen Einstellungen ausgeliefert und ist nur bedingt von der einsetzenden Stelle anpassbar
1.7 Sonstige Anforderungen	entfällt	
Komplex 2:		
2.1.1 Gesetzliche Ermächtigung zur Verarbeitung der Daten	vorbildlich	
2.1.2 Einwilligung des Betroffenen	adäquat	Eine gesonderte Einwilligung des Betroffenen in die Speicherung in einem externen Rechenzentrum ist wegen der verwendeten Verschlüsselungsverfahren nicht erforderlich.
2.1.3.1 Vorschriften über die Datenerhebung	entfällt	

Anforderung nach Katalog oder sonstigen Rechtsnormen	**Bewertung**	**Kommentare**
2.1.3.2 Vorschriften über die Übermittlung	entfällt	
2.1.3.3 Löschung nach Wegfall des Erfordernisses	entfällt	
2.2.1 Zweckbindung und Zweckänderung	vorbildlich	
2.2.2 Erleichterung der Umsetzung des Trennungsgebotes	entfällt	
2.2.3 Gewährleistung der Datensicherheit (§§ 5, 6 LDSG, Anlage zu § 9 BDSG)	adäquat	
2.3 Datenverarbeitung im Auftrag	adäquat	
2.4.1 gemeinsame Verfahren/Abrufverfahren	entfällt	-
2.4.2 Trennung der Verantwortlichkeiten	entfällt	-
2.4.3 Veröffentlichungen im Internet	entfällt	
2.4.4 Weitere besondere technische Verfahren	entfällt	
2.5.1 Erleichterung bzw. Unterstützung von Pseudonymität und des Pseudonymisierens	adäquat	Es werden sowohl Verschlüsselungs-, als auch Pseudonymisierungsverfahren eingesetzt
Komplex 3:		
3.1.1. Physikalische Sicherung	adäquat	
3.1.2 Authentisierung	adäquat	
3.1.3 Autorisierung	vorbildlich	
3.1.4 Protokollierung	vorbildlich	
3.1.5 Verschlüsselung und Signatur	vorbildlich	
3.1.6 Pseudonymisieren	adäquat	
3.1.7 Anonymisieren	entfällt	
3.2.1.1 Verfügbarkeit	adäquat	Sofern auf das Rechenzentrum (als Auftragsdatenverarbeiter) bezogen
3.2.1.2 Integrität	vorbildlich	Durch die Verschlüsselung gegeben

Anforderung nach Katalog oder sonstigen Rechtsnormen	**Bewertung**	**Kommentare**
3.2.1.3 Vertraulichkeit	vorbildlich	
3.2.1.4 Nicht-Verkettbarkeit	adäquat	Durch den Einsatz von Pseudonymisierungsverfahren
3.2.1.5 Transparenz	adäquat	
3.2.1.6 Intervenierbarkeit	adäquat	
3.2.1.7 Protokollierung von Datenverarbeitungsvorgängen	adäquat	
3.2.1.8 Test und Freigabe	adäquat	Es gibt eine Testplattform für einsetzende Stellen und Änderungen werden Transparent dargestellt.
3.2.2 Erleichterung der Vorabkontrolle	adäquat	
3.2.3 Erleichterung bei der Erstellung des Verfahrensverzeichnisses	adäquat	
3.2.4 Benachrichtigungspflicht bei unrechtmäßiger Kenntniserlangung von Daten	entfällt	
3.2.5 Unterstützung der Tätigkeit des behördlichen Datenschutzbeauftragten	entfällt	
3.3.1 Verschlüsselung	vorbildlich	
3.3.2 Anonymisierung oder Pseudonymisierung	adäquat	
3.3.3.1 Mobile Datenverarbeitungssysteme	entfällt	
3.3.3.1 Video-Überwachung und –Aufzeichnung	entfällt	
3.3.3.1 Automatisierte Einzelentscheidungen	entfällt	
3.3.3.1 Veröffentlichungen im Internet	entfällt	
3.4 Pflichten nach Datenschutzverordnung (DSVO), insbesondere für Verfahren	adäquat	
3.5 Anforderungen an den Betrieb bei Auftragsdatenverarbeitung	adäquat	
3.6 Sonstige Anforderungen	entfällt	

Anforderung nach Katalog oder sonstigen Rechtsnormen	Bewertung	Kommentare
Komplex 4:		
4.1 Aufklärung und Benachrichtigung	adäquat	Ist jederzeit durch die verantwortliche Stelle möglich.
4.2 Benachrichtigung des Betroffenen bei unrechtmäßiger Kenntniserlangung von Daten	adäquat	Ist jederzeit durch die verantwortliche Stelle möglich.
4.3 Auskunft	adäquat	Ist jederzeit durch die verantwortliche Stelle möglich.
4.4.1 Berichtigung	adäquat	Ist jederzeit durch die verantwortliche Stelle möglich.
4.4.2 Vollständige Löschung	adäquat	Kann durch die verantwortliche Stelle angestoßen werden. Die endgültige Löschung ist erfolgt, wenn die Datenbanken ordnungsgemäß repliziert sind.
4.4.3 Sperrung	adäquat	Eine Sperrung kann über das Rechtesystem realisiert werden.
4.4.4 Einwand bzw. Widerspruch gegen die Verarbeitung	adäquat	
4.3.5 Gegendarstellung	adäquat	
4.5 Sonstige Anforderungen	entfällt	

E. Wie das Produkt den Datenschutz fördert

Die Stärke des Produktes liegt in der sofortigen Verschlüsselung der Daten, die noch auf dem Client stattfindet, also noch vor der Übertragung und Speicherung.

Somit ist es nur der datenverarbeitenden Stelle möglich, die Daten mit Personenbezug zu lesen, nicht aber Dritten, wie dem Hersteller oder seinen Dienstleistern. Das heißt, sobald ein Feld ein identifizierbares Datum enthalten kann wird das Feld verschlüsselt. Darüber hin-

aus werden alle auch alle anderen Daten, die der Schweigepflicht des § 203 StGB unterliegen, verschlüsselt.
Insgesamt gibt es keine unverschlüsselten Felder, die patientenidentifizierende Daten enthalten können.

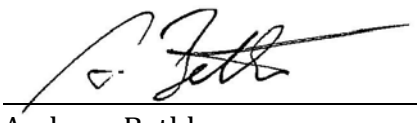
In Punkto Transparenz geht der Hersteller über das normale Maß hinaus und liefert seinen clientseitigen Programmcode in lesbarer Form mit aus. Darüber hinaus hat der Hersteller in seiner Dokumentation beschrieben, wie der Anwender die Verschlüsselungsmodule selbst auf Manipulationsfreiheit hin überprüfen kann.

F. Zusammenfassung

Insgesamt kann festgestellt werden, dass auch mit dem neuen Produkt die Rechtsvorschriften zu Datenschutz und Datensicherheit eingehalten werden.

Hiermit bestätige ich, dass das oben genannte IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht.

Kellinghusen, den 13.12.2016



Andreas Bethke

Flensburg, den 13.12.2016

Stephan Hansen-Oest