stratego IT

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN VON GDD UND BVD

Bericht

zum Zertifizierungsaudit nach
DATENSCHUTZSTANDARD DS-BVD-GDD-01
"Anforderungen an Auftragnehmer nach § 11 BDSG"

für

Deutsche Telekom Healthcare and Security Solutions GmbH, eine Tochter der T-Systems International GmbH

über die Leistungen
–
Study Based Archiving Service „StArcS “ –
PACS Langzeitarchivierung –

AUDITOR
ZUR PRÜFUNG NACH
DS-BVD-GDD-01
GÜLTIG BIS
28.07.2017

Berichtersteller	Stefan Staub
DSZ-Zulassungs-Nr.	Z-009
Anschrift	stratego IT management GmbH Hofäckerstraße 32 D-74374 Zaberfeld
Berichts-Datum	10.10.2015

Inhaltsverzeichnis

1. Einführung ... 3
1.1. Ziel des Audits ... 3
1.2. Anwendungsbereich der Zertifizierung Reg.Nr. [DSZ-Zertifizierungs-Nummer] ... 4
2. Management Summary / Zusammenfassung ... 4
3. Obligatorische Anforderungen / Scoping ... 6
3.1. Prüfungsrelevante Kernmodule ... 6
3.2. Prüfungsrelevante Module in Abhängigkeit des Leistungsumfangs ... 7
3.3. Genehmigte Ausnahmen ... 7
4. Auditierte Bereiche & Feststellungen ... 7
4.1. Kernmodule: ... 7
4.1.1. Leistungsbeschreibung ... 7
4.1.2. Herstellung ... 8
4.1.3. Datenschutzkonzept ... 9
4.1.4. IT-Sicherheitskonzept ... 11
4.1.5. Managementsysteme ... 13
4.2. Module in Abhängigkeit des Leistungsumfangs ... 14
5. Audit Teilnehmer ... 15
6. Prüfergebnis / Prüfvermerk ... 15
Bemerkungen der DSZ ... 17

1. Einführung

Dieser Bericht wurde von Stefan Staub erstellt und beschreibt die Tätigkeiten bzgl. unten stehender Auditaktivitäten:

Organisation	Erstprüfung / Verlängerung	Audittermin (Start)
Deutsche Telekom Healthcare and Security Solutions GmbH, eine Tochter der T-Systems International GmbH Pascalstr. 11 (Geschäftsanschrift) Friedrich-Ebert-Allee 140 (Sitz der Gesellschaft) 10587 Berlin (Geschäftsanschrift) 53113 Bonn (Sitz der Gesellschaft)	x Erstprüfung ☐ Verlängerung	06.08.2015

1.1. Ziel des Audits

Das Ziel des Audits war eine Überprüfung der im Anwendungsbereich beschriebenen Leistung, um zu gewährleisten, dass die im Anwendungsbereich getroffenen Maßnahmen und erforderlichen Umsetzungen nach dem DATENSCHUTZSTANDARD DS-BVD-GDD-01 "Anforderungen an Auftragnehmer nach § 11 BDSG" und sonstigen Vorgaben der Zertifizierungsgesellschaft erfüllt werden. Es mündet in der Empfehlung hinsichtlich einer Zertifizierung.

Das Audit mit dem Ziel der Zertifizierung nach dem DATENSCHUTZSTANDARD DS-BVD-GDD-01 "Anforderungen an Auftragnehmer nach § 11 BDSG" dient folgenden Aspekten:

- Auftraggeber können die Zertifizierung ihrem eigenen Kontrollermessen gemäß § 11 Abs. 2 BDSG zugrunde legen.
- Das Unternehmen signalisiert als Auftragnehmer sein gesetzeskonformes Datenschutzniveau.

Dieses Vor-Ort durchgeführte Audit basiert auf Stichproben. Es kann somit nicht ausgeschlossen werden, dass Abweichungen nicht erkannt werden.

Wenn Sie diesen Auditbericht an Dritte weiterleiten möchten, sind alle Teile des Berichtes zu übermitteln. Auszüge oder Teile des Berichts dürfen nicht an Dritte weitergeleitet werden.

1.2. Anwendungsbereich der Zertifizierung Reg.Nr. A-002

Ort	Auditierte Leistung
Deutsche Telekom AG Dingolfinger Str. 1-15 81673 München	Study Based Archiving Service „StArcS" – PACS Langzeitarchivierung inkl. Altdatenmigration

Bei der "StArcS" Langzeitarchivierung der PACS Bilddaten werden die Daten in Rechenzentren der Deutschen Telekom katastrophensicher gespiegelt archiviert. Die Archivierung beinhaltet die regelmäßige Migration der Daten auf neue Speichermedien ebenso wie eine langfristig sichere Verschlüsselung ohne zusätzliche Kosten für den Kunden.

Dem Kunden wird ein Preismodell „pay per study" vorgeschlagen. Hierbei zahlt er einmalig für eine 10jährige Archivierung je archivierter Studie. Die Daten der laufenden Produktion werden hierbei online über eine VPN Verbindung an ein Rechenzentrum der Deutschen Telekom/T-Systems übertragen. Die Übertragung der Daten basiert auf der standardisierten DICOM-Kommunikation ohne proprietäre Zusatzfunktionen

Für die Übertragung der bereits im System des Kunden vorhandenen Altdaten werden – je nach verfügbarer Bandbreite und gewünschtem Migrationszeitraum – zwei alternative Modelle vorgeschlagen.

1. Online-Übertragung: hierbei wird im Wesentlichen der oben beschriebene Workflow aufgegriffen, benötigt wird hierfür eine entsprechende Konfiguration im PACS („Push-Migration")
2. Offline-Übertragung: hierbei werden die Daten zunächst lokal auf ein geeignetes Speichermedium übertragen. Das Speichermedium wird in der Folge physisch in ein Datenzentrum der deutschen Telekom verbracht und dort die Daten eingespielt.

Bei mehreren Leistungen:

☐ Der vorliegende Bericht ist der Referenzbericht

☐ Der vorliegende Bericht ist nur gültig im Zusammenhang mit dem Referenzbericht: _____. Er beschränkt sich im Folgenden auf abweichende Feststellungen.

2. Management Summary / Zusammenfassung

Zunächst darf ich mich bei allen Beteiligten und Verantwortlichen für die gute Zusammenarbeit, die exzellente Vorbereitung und offene Kommunikation während des Auditprozesses bedanken.

Die in diesem Audit geprüfte Leistung „Study Based Archiving Service“ und die dazugehörige Organisation entspricht in vollem Umfang den entsprechenden Anforderungen des §11 BDSG „Datenverarbeitung im Auftrag“ und den Vorgaben und Anforderungen des Standards DSZ-BvD-GDD-001, sowie den unternehmenseigenen Richtlinien und Vorgaben bzgl. des technischen und organisatorischen Datenschutzes.

Es wurden keine Abweichungen festgestellt.
Insbesondere die organisatorischen Maßnahmen sowie die Dokumentation sind im Kontext des Konzerns integriert und stehen allen Beteiligten jederzeit zur Verfügung.
Die technischen Maßnahmen wurden anhand der bestehenden Prozesse, Dokumente und Zertifikate überprüft und genügen vollumfänglich dem aktuellen Stand der Technik.

Eine festgestellte Beobachtung:
Die Dokumentation, sowie die notwendigen Kontrollprozesse haben einen sehr hohen methodischen Reifegrad. Hier sollte im kommenden Jahr kritisch hinterfragt werden, ob dies unter Effizienzgesichtspunkten an allen Stellen in dieser Tiefe wirklich notwendig ist. Es ist zu erwarten, dass dies unter anderem im Security Maßnahmenprogramm 2016 aufgenommen wird.
Die hierzu bereits geplanten Analysen sollten im nächsten Überprüfungsaudit entsprechende Ergebnisse zur Verfügung stellen.
Positiv hervorzuheben ist das ehemalige Projekt „Herstellung der Compliance bei der Datenverarbeitung für Kunden im Auftrag“ (Ergebnis: ADV-Framework), welches nun innerhalb der T-Systems International GmbH und den in das Prozessmodel integrierten Töchtern in einen Regelprozess überführt wurde.
Im Zuge dieses Prozesses werden die Anforderungen des §11 BDSG und alle weiteren Anforderungen des Unternehmens sichergestellt. Im Rahmen des kontinuierlichen Verbesserungsprozesses sollte die Möglichkeit eines konzernweiten Rollouts überprüft werden.

3. Obligatorische Anforderungen / Scoping

3.1. Prüfungsrelevante Kernmodule

Modul			relevant
4.1 Leistungsbeschreibung	4.1.1	Beschreibung der Leistung	**Ja**
	4.1.2	Beschreibung der Auftragsbearbeitung (Herstellung)	**Ja**
4.2 Input-Management			**Ja**
4.3 Auftragsmanagement			**Ja**
4.4 Output-Management			**Ja**
4.5 Datenschutzkonzept	4.5.1	Eingabekontrolle	**Ja**
	4.5.2	Trennungsgebot	**Ja**
	4.5.3	Auftragskontrolle	**Ja**
	4.5.4	Prozessbeschreibung Auskunft	**Ja**
	4.5.5	Prozessbeschreibung Berichtigung	**Ja**
	4.5.6	Prozessbeschreibung Sperrung	**Ja**
	4.5.7	Prozessbeschreibung Löschung	**Ja**
	4.5.8	Prozessbeschreibung Sicherheitsvorfall	**Ja**
4.6 IT-Sicherheitskonzept	4.6.2.1	Erstellung und Verwendung des IT-Sicherheitskonzepts	**Ja**
	4.6.2.2	Mindeststandard Gebäudesicherheit	**Ja**
	4.6.2.3	Mindeststandard Zutrittsschutz	**Ja**
	4.6.2.4	Mindeststandard Zugangsschutz	**Ja**
	4.6.2.5	Mindeststandard Zugriffsschutz	**Ja**
	4.6.2.6	Mindeststandard Verfügbarkeit	**Ja**
	4.6.2.7	Mindeststandard Datenübertragung	**Ja**
4.7 Datenschutz-Managementsystem	4.7.4.1	Der Datenschutzbeauftragte	**Ja**
	4.7.4.2	Kontrolle des Datenschutzkonzeptes	**Ja**
	4.7.4.3	Kontrolle der Unterauftragnehmer	**Ja**
4.8 IT-Sicherheitsmanagementsystem			**Ja**
4.9 Auftragsmanagementsystem			**Ja**

3.2. Prüfungsrelevante Module in Abhängigkeit des Leistungsumfangs

Modul		relevant
5.1 Vertrag		**Ja**
5.2 Beendigung der Leistungsbeziehung		**Ja**

3.3. Genehmigte Ausnahmen

Laut Antragstellung wurde die Begehung des Rechenzentrums ausgeschlossen. Es bestehen ausreichend gültige und aussagefähige Zertifikate, um die Einhaltung der notwendigen technischen und organisatorischen Maßnahmen zu belegen. Es wurden weiterhin Interviews mit Verantwortlichen des Rechenzentrums geführt.

Durch die klar und eng abgegrenzte Leistung wurde einer Reduzierung des Auditumfangs um 8 Std. stattgegeben.

4. Auditierte Bereiche & Feststellungen

4.1. Kernmodule:

Die Beschreibung liegt sowohl in interner als auch in extern verfügbarer Form vor.

Bei der Beantragung des Produktes/ der Leistung müssen interne Prozesse durchlaufen werden, welche eine präzise Beschreibung notwendig machen.

Im vorgelegten Kundenprospekt wird die Leistung hinreichend beschrieben.

4.1.1. Leistungsbeschreibung

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.1.1 Beschreibung der Leistung	Liegt schriftlich dokumentiert und in ausreichendem Umfang vor.
Prüfmethode / Prüfhandlung	
In der Dokumentenprüfung, als auch in der individuellen Auditsitzung konnten die Verantwortlichen die genannten Anforderungen vollumfänglich nachweisen (PowerPoint Präsentation, gedruckte Prospekte, Darstellung des Genehmigungsprozesses).	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.1.2 Beschreibung der Herstellung	Liegt schriftlich dokumentiert und in ausreichendem Umfang vor.
Prüfmethode / Prüfhandlung	
Durch Einbettung in die Standardprozesse des Konzerns sind im Genehmigungsprozess ausführliche Beschreibungen gefordert, die dem Auditor vorlagen und mündlich erläutert wurden.	

4.1.2. Herstellung

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.2 Input-Management	Durch die Standardisierung und den eng gefassten Produktumfang werden die Anforderungen durch interne Regelprozesse vollumfänglich abgebildet.
Prüfmethode / Prüfhandlung	
Einsicht in die Dokumentation, der workflowgestützten Werkzeuge des Konzerns und des Dokumentenmanagementsystems sowie Intranet/Wikis und Erläuterungen der jeweiligen Verantwortlichen konnte die ausreichende und effektive Umsetzung der Anforderungen geprüft und festgestellt werden.	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.3 Auftragsmanagement	Durch die Standardisierung und des eng gefassten Produktumfangs werden die Anforderungen durch interne Regelprozesse vollumfänglich abgebildet.
Prüfmethode / Prüfhandlung	
Einsicht in die Dokumentation, der workflowgestützten Werkzeuge des Konzerns und des Dokumentenmanagementsystems sowie Intranet/Wikis und Erläuterungen der jeweiligen Verantwortlichen konnte die ausreichende und effektive Umsetzung der Anforderungen geprüft und festgestellt werden.	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.4 Output-Management	Durch die Standardisierung und des eng gefassten Produktumfangs werden die Anforderungen durch interne Regelprozesse vollumfänglich abgebildet.
Prüfmethode / Prüfhandlung	
Einsicht in die Dokumentation, der workflowgestützten Werkzeuge des Konzerns und des Dokumentenmanagementsystems sowie Intranet/Wikis und Erläuterungen der jeweiligen Verantwortlichen konnte die ausreichende und effektive Umsetzung der Anforderungen geprüft und festgestellt werden.	

4.1.3. Datenschutzkonzept

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.5.1 Eingabekontrolle	Durch interne Vorgaben bei der Datenverarbeitung und Nutzung des Rechenzentrums werden Zugriffe und Änderungen im System vollständig protokolliert
Prüfmethode / Prüfhandlung	
Die jeweiligen Verantwortlichkeiten konnten plausibel die Prozesse und Workflows, sowie technische Maßnahmen erläutern.	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.5.2 Trennungsgebot	Die technische Umsetzung einer Mandantentrennung ist nach dem Stand der Technik erfolgt.
Prüfmethode / Prüfhandlung	
Die jeweiligen Verantwortlichkeiten konnten plausibel die Prozesse und Workflows, sowie technische Maßnahmen erläutern.	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.5.3 Auftragskontrolle	Entsprechende Standardprozesse garantieren unternehmensweit die Verfolgung und Steuerung von Aufträgen seitens der Auftraggeber. Für die auditierte Leistung steht jedoch eine individuelle Anpassung an den Kunden nicht zur Verfügung. Der Auftraggeber kauft die Leistung wie beschrieben ein. Lediglich Speicherumfang und Vertragslaufzeit sind erweiterbar.
Prüfmethode / Prüfhandlung	
Die jeweiligen Verantwortlichkeiten konnten plausibel die Prozesse und Workflows, sowie technische Maßnahmen erläutern. Eine Einsicht in Workflowtools war in ausreichender Tiefe vorhanden.	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.5.4 Prozessbeschreibung Auskunft	Der Auftraggeber ist durch die technischen Maßnahmen per se immer in der Lage auf alle gespeicherten Daten selbständig zuzugreifen. Ein Eingriff seitens des Leistungserbringers ist nicht notwendig und erfolgt nicht.

Prüfmethode / Prüfhandlung
Die jeweiligen Verantwortlichkeiten konnten plausibel die Prozesse und Workflows, sowie technische Maßnahmen erläutern. Eine Einsicht in Workflowtools und Dokumente war in ausreichender Tiefe vorhanden.

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.5.5 Prozessbeschreibung Berichtigung	Die Daten werden durch Standardkommunikation im Bereich der medizinischen Bilddaten erfasst, transportiert und gespeichert. Die Kontrolle erfolgt dabei direkt durch den Auftraggeber. Die technische Basis, insbes. die eingesetzte Hardware unterliegt permanentem Monitoring nach dem Stand der Technik.
Prüfmethode / Prüfhandlung	
Die jeweiligen Verantwortlichkeiten konnten plausibel die Prozesse und Workflows, sowie technische Maßnahmen erläutern. Eine Einsicht in Workflowtools und Dokumente war in ausreichender Tiefe vorhanden.	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.5.6 Prozessbeschreibung Sperrung	Da die Daten lediglich vom Auftraggeber genutzt werden können und eine Sperrung nicht in der Natur der Bildarchivierung liegt, gibt es hierzu keine weiteren Maßnahmen.
Prüfmethode / Prüfhandlung	
Die jeweiligen Verantwortlichkeiten konnten plausibel die Prozesse und Workflows, sowie technische Maßnahmen erläutern. Eine Einsicht in Workflowtools und Dokumente war in ausreichender Tiefe vorhanden.	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.5.7 Prozessbeschreibung Löschung	Die Daten werden vertragsgemäß gespeichert und nach Vertragsende datenschutzkonform gelöscht. Die Löschung erfolgt durch Standardtools im RZ. Die Entsorgung von Festplatten und Speichermedien entspricht dem Regelprozess für die Entsorgung von Medien.
Prüfmethode / Prüfhandlung	
Die jeweiligen Verantwortlichkeiten konnten plausibel die Prozesse und Workflows, sowie technische Maßnahmen erläutern. Eine Einsicht in Workflowtools und Dokumente war in ausreichender Tiefe vorhanden. Insbes. der Prozess der Entsorgung von Datenträgern wurde durch gesonderte Dokumente und Prozesse, sowie das ADV-Framework und die Überprüfung von ext. Dienstleistern und deren Zertifizierungen hinreichend tief geprüft.	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.5.8 Prozessbeschreibung Sicherheitsvorfall	Die adäquate Behandlung von etwaigen Sicherheitsvorfälle wird durch die unternehmensweiten Incidentmanagement-Prozesse sichergestellt.
Prüfmethode / Prüfhandlung	
Die jeweiligen Verantwortlichkeiten konnten plausibel die Prozesse und Workflows, sowie technische Maßnahmen erläutern. Eine Einsicht in Workflowtools und Dokumente war in ausreichender Tiefe vorhanden.	

4.1.4. IT-Sicherheitskonzept

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.6.2.1 Erstellung und Verwendung des IT-Sicherheitskonzepts	Konzernweite Sicherheitsstrukturen und Umsetzung der internationalen Standards wie ISO27001, ISO22301 und weiterer Normen der Wirtschaftsprüfer, sowie eigene Unternehmensabteilungen garantieren ein durchgängiges Sicherheitskonzept.
Prüfmethode / Prüfhandlung	
Die jeweiligen Verantwortlichkeiten konnten plausibel die Prozesse und Workflows, sowie technische Maßnahmen erläutern. Eine Einsicht in Workflowtools und Dokumente war in ausreichender Tiefe vorhanden.	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.6.2.2 Mindeststandard Gebäudesicherheit	Konzernweite Sicherheitsstrukturen und Umsetzung der internationalen Standards wie ISO27001, ISO22301 und weiterer Normen der Wirtschaftsprüfer, sowie eigene Unternehmensabteilungen garantieren ein durchgängiges Sicherheitskonzept.
Prüfmethode / Prüfhandlung	
Die jeweiligen Verantwortlichkeiten konnten plausibel die Prozesse und Workflows, sowie technische Maßnahmen erläutern. Eine Einsicht in Workflowtools und Dokumente war in ausreichender Tiefe vorhanden. Eine Begehung am Standort München verlief ohne Abweichungsfeststellung.	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.6.2.3 Mindeststandard Zutrittsschutz	Konzernweite Sicherheitsstrukturen und Umsetzung der internationalen Standards wie ISO27001, ISO22301 und weiterer Normen der Wirtschaftsprüfer, sowie eigene Unternehmensabteilungen garantieren ein durchgängi-

	ges Sicherheitskonzept. Der Zutrittsschutz erfolgt durch standardisierte Zutrittskontrollmechanismen (elektronische Kontrolle mittels Mitarbeiterausweis),Pförtner/Empfang und Zwiebelprinzip bzgl. der Zugänglichkeit der Bereiche (Kundenbereiche, interne Bereiche, Rechenzentrum)
Prüfmethode / Prüfhandlung	
Die jeweiligen Verantwortlichkeiten konnten plausibel die Prozesse und Workflows, sowie technische Maßnahmen erläutern. Eine Einsicht in Workflowtools und Dokumente war in ausreichender Tiefe vorhanden. Eine Begehung am Standort München verlief ohne Abweichungsfeststellung.	

Prüfaspekt im Standard /Anforderung	**Feststellung / Befund**
4.6.2.4 Mindeststandard Zugangsschutz	Login Verfahren werden unternehmensweit technisch durchgesetzt. Hierzu gehören: Individuelle Benutzer, komplexe Passworte und Änderung im regelmäßigen, erzwungenen Rhythmus.
Prüfmethode / Prüfhandlung	
Die jeweiligen Verantwortlichkeiten konnten plausibel die Prozesse und Workflows, sowie technische Maßnahmen erläutern. Eine Einsicht in Workflowtools und Dokumente war in ausreichender Tiefe vorhanden. Eine Begehung am Standort München verlief ohne Abweichungsfeststellung.	

Prüfaspekt im Standard /Anforderung	**Feststellung / Befund**
4.6.2.5 Mindeststandard Zugriffsschutz	Zentrale Vergabe von Benutzern, ink. Changemanagement mittels eines zentralen Rollen- und Benutzerkonzeptes anhand interner Richtlinien und Arbeitsanweisungen.
Prüfmethode / Prüfhandlung	
Die jeweiligen Verantwortlichkeiten konnten plausibel die Prozesse und Workflows, sowie technische Maßnahmen erläutern. Eine Einsicht in Workflowtools und Dokumente war in ausreichender Tiefe vorhanden. Eine Überprüfung am Standort München verlief ohne Abweichungsfeststellung.	

Prüfaspekt im Standard /Anforderung	**Feststellung / Befund**
4.6.2.6 Mindeststandard Verfügbarkeit	Es gelten die allgemeinen Standards des Unternehmens bzgl. Verfügbarkeit. Während des internen Genehmigungsprozesses werden konkrete Anforderungen definiert. Diese werden im Rechenzentrum anforde-

	rungsgerecht umgesetzt und überwacht. Es handelt sich um hochverfügbare DV-Einheiten mit einem Backupkonzept zur Langzeitarchivierung auf optischen Speichermedien.
Prüfmethode / Prüfhandlung	
Die jeweiligen Verantwortlichkeiten konnten plausibel die Prozesse und Workflows, sowie technische Maßnahmen erläutern. Eine Einsicht in Workflowtools und Dokumente war in ausreichender Tiefe vorhanden.	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.6.2.7 Mindeststandard Datenübertragung	Die Datenübertragung erfolgt mittels DICOM Standard und über eine verschlüsselte Verbindung (VPN).
Prüfmethode / Prüfhandlung	
Die jeweiligen Verantwortlichkeiten konnten plausibel die Prozesse und Workflows, sowie technische Maßnahmen erläutern. Eine Einsicht in Workflowtools und Dokumente war in ausreichender Tiefe vorhanden. Eine Einsicht in die Beschreibung der technischen Vorgaben ergab keine Anhaltspunkte über Schwachpunkte der Kommunikation.	

4.1.5. Managementsysteme

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.7 Datenschutz-Managementsystem	Datenschutz wird durch die durchgehenden Konzernstrukturen und Prozesse sichergestellt. Hierbei wird zwischen der strategischen Abteilung Group Privacy des Datenschutzbeauftragten (Zuständig für rechtliche Vorgaben, inhaltliche Prozessvorgaben und Governance), den divisionsspezifischen Brückenköpfen sowie dezentralen Koordinatoren in den jeweiligen Verantwortungsbereichen und den Umsetzungsverantwortlichen (Themen/Produktverantwortliche) unterschieden.
Prüfmethode / Prüfhandlung	
Die jeweiligen Verantwortlichkeiten konnten plausibel die Prozesse und Workflows, sowie technische Maßnahmen erläutern. Eine Einsicht in Workflowtools und Dokumente war in ausreichender Tiefe vorhanden. Eine separate Auditeinheit mit Mitarbeitern der Group Privacy und den Brückenköpfen in der Organisation konnte die dokumentierte Sachlage bestätigen.	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.8 IT-Sicherheitsmanagementsystem	Analog zum Datenschutzmanagement besteht eine eigene Organisationsstruktur für IT-Sicherheit.

Prüfmethode / Prüfhandlung
Die jeweiligen Verantwortlichkeiten konnten plausibel die Prozesse und Workflows, sowie technische Maßnahmen erläutern. Eine Einsicht in Workflowtools und Dokumente war in ausreichender Tiefe vorhanden. Eine separate Auditeinheit mit Mitarbeitern der Sicherheitsorganisation und den Brückenköpfen in der Organisation konnte die dokumentierte Sachlage bestätigen.

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
4.9 Auftragsmanagementsystem	Das eingeführte ADV-Framework, welches erfolgreich in einen Regelprozess überführt wurde, stellt umfangreich die Maßgaben des §11 BDSG sicher.
Prüfmethode / Prüfhandlung	
Die jeweiligen Verantwortlichkeiten konnten plausibel die Prozesse und Workflows, sowie technische Maßnahmen erläutern. Eine Einsicht in Workflowtools und Dokumente war in ausreichender Tiefe vorhanden. Eine separate Auditeinheit mit Verantwortlichen des ADV-Frameworks konnte die dokumentierte Sachlage bestätigen.	

4.2. Module in Abhängigkeit des Leistungsumfangs

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
5.1 Vertrag	Da es sich um einen fest definierten Leistungsumfang handelt werden standardisierte Verträge, SLAs und Vertragsanhänge zur ADV genutzt. Hierbei kommt der interne Prozess zur Absicherung von Anforderungen bzgl. des §11 BDSG zum Tragen.
Prüfmethode / Prüfhandlung	
Einsicht in die Standardprozesse, Mustervertrag, ADV-Mustervertrag.	

Prüfaspekt im Standard /Anforderung	Feststellung / Befund
5.2 Beendigung der Leistungsbeziehung	Die Beendigung erfolgt durch die definierte Vertragslaufzeit. Hierbei wird workflowgesteuert der Löschvorgang initiiert. Vor Ablauf des Vertrages wird der Auftraggeber über die bevorstehende Löschung informiert. Der Auftraggeber hat die Möglichkeit selbst die Daten in seinen Wirkungsbereich zu übertragen und/oder den Vertrag zu verlängern.
Prüfmethode / Prüfhandlung	
Einsicht in die Verträge und Erläuterung der Prozesse durch den Produktverantwortlichen.	

5. Audit Teilnehmer

Beteiligte Stellen / Unterauftragnehmer / Dienstleister / sonstige Dritte

Name / Adresse	Aufgabe bei der Leistungserbringung
Deutsche Telekom Healthcare and Security Solutions GmbH	Strategy & Products – Portfolio Kliniken Service – Service Kliniken & Kassen
T-Systems International GmbH	Data & IT Security – Global Information Security Management System Security, Compliance & Quality Management – Licence & Asset Management (IT Division – Quality) CSS Audit & Compliance Management – Compliance Management (Global IT Operations – Quality CSS) Global MoD – Global Problem Management (IT Division – Quality)
Deutsche Telekom AG – Group Headquarter	Group Privacy – Business, Services & Infrastructure

6. Prüfergebnis / Prüfvermerk

Es konnten alle Bereiche wie geplant auditiert werden.
Genehmigte Ausnahme war das betroffene Rechenzentrum. Hier wurde aufgrund zahlreicher gültiger Zertifikate von einer Begehung abgesehen. Die Prozesse wurden durch Interviews und Dokumentensichtung in ausreichender Tiefe geprüft.
Ebenso besteht aufgrund der Eigenschaften der überprüften Leistung eine automatische Löschung der archivierten Daten nach Beendigung des Vertragsverhältnisses. Die Lösch- sowie die Entsorgungsprozesse wurden auditiert. Der Auftraggeber hat während der gesamten Vertragslaufzeit vollen Zugriff auf die archivierten Bilddaten.
Die sehr eng umrissene Leistung der Langzeitarchivierung von radiologischen Bildern ist in vollem Umfang in die bereits bestehenden Prozesse des Konzerns der Deutschen Telekom bzw T-Systems International GmbH und der verantwortlichen Gesellschaft Deutsche Telekom Healthcare and Security Solutions GmbH eingebettet.
Anforderungen des §11 BDSG werden durch die Standardprozesse umfänglich abgebildet. Hierbei dient der Regelprozess innerhalb des ADV-Frameworks als tragendes Element und

führt und steuert effektiv die besonderen Anforderungen der Datenverarbeitung im Auftrag, sowie der Anforderungen des Standards DS-BvD-GDD-001 in der T-Systems International GmbH und der Deutsche Telekom Healthcare and Security Solutions GmbH und somit auch in der auditierten Leistungserbringung.
Potentielle Auftraggeber können somit im Sinne des Standards DS-BvD-GDD-001 auf die geforderten technischen und organisatorischen Maßnahmen vertrauen.

Ich empfehle hiermit die Erteilung des Siegels für die Leistung:

Study Based Archiving Service „StArcS“ – PACS Langzeitarchivierung

Bemerkungen der DSZ

Das Siegel wird erteilt

Ja

Nummer des Zertifikats:

U-002

Gültigkeit des Zertifikats:

24.11.2017