



Zertifikat

Die **datenschutz cert** GmbH bestätigt hiermit
als Ergebnis der Zertifizierungsentscheidung gemäß Art. 42 Abs. 5 DSGVO, dass die

Siemens Healthineers AG
Siemensstraße 3, 91301 Forchheim

die Datenverarbeitung
Dienste der cloudbasierten Plattform teamplay
gemäß Anlage

als Auftragsverarbeiter gemäß Art. 4 Nr. 8 DSGVO innerhalb des Geltungsbereichs: D

konform zu den Anforderungen der EU-Verordnung 2016/679 (DSGVO) und den
zusätzlichen Anforderungen der Datenschutzaufsichtsbehörden betreibt und dies
innerhalb der Laufzeit des Zertifikats auf Konformität überwacht wird. Die Gründe für
die Erteilung des Zertifikats wurden der Datenschutzaufsichtsbehörde Bremen gemäß
Art 43 Abs. 5 DSGVO am 15.10.2025 mitgeteilt.

Prüfgrundlagen
Konformitätsbewertungsprogramm zur Zertifizierung einer IT-gestützten
Verarbeitung personenbezogener Daten gem. Art. 42 DSGVO („DSGVO – information
privacy standard“) Version 1.0
Kriterienkatalog zur Zertifizierung einer IT-gestützten Verarbeitung personen-
bezogener Daten gem. Art. 42 DSGVO („DSGVO – information privacy standard“)
Version 1.0.



Zertifikats-ID: **DSC.1614.10.2025**
Abschluss der Evaluierung: **15.09.2025**
Zertifizierungsentscheidung: **23.10.2025**
Datum der Ausstellung: **23.10.2025**
Überwachung: **nächste geplante Überwachung 12/24 Monate**
nach dem Abschluss der Evaluierung
Laufzeit bis: **21.10.2028**

datenschutz
■ ■ ■ **cert**

Dr. Sönke Maseberg
Leiter der Zertifizierungsstelle



Anhang zum Zertifikat mit der Zertifikats- ID DSC.1614

Anlage 1

Zertifizierungsdetails

Geltungsbereich

Kontaktdaten des Kunden:

Siemens Healthineers AG, Siemensstr. 3, 91301 Forchheim

Beschreibung der Datenverarbeitung:

Dienste der cloudbasierten Plattform teamplay

Branche:

Gesundheitswesen

Dienstleistungserbringung als

Auftragsverarbeiter

SOA-Dokument:

SHC, ZV59c_ips-DSGVO_Referenzdokumentation v1.2_SHS, Version 1.2 vom 18.08.2025

Kurzbeschreibung der Datenverarbeitung:

teamplay ist eine cloudbasierte Plattform mit verschiedenen Diensten, um Gesundheitseinrichtungen bei der Verbesserung ihrer bildgebenden Verfahren und klinischen Arbeitsabläufe zu unterstützen. Das Einsatzgebiet der Plattform ist der Gesundheitssektor; teamplay ist für die Verwendung durch medizinisches Fachpersonal bestimmt. Dies umfasst:

- teamplay Performance Management Anwendungen
 - teamplay Dose
 - teamplay Usage
 - teamplay Protocols
 - teamplay Contrast
 - teamplay Insights
- Modality Dashboards
 - teamplay MR Dashboard
 - teamplay CT Dashboard
 - teamplay X-Ray Dashboard
- AI-Rad Companion (AIRC) (inklusive dem AIRC Notifier)
- Administrative Anwendungen
 - teamplay Admin Center sowie
 - teamplay Receiver + AIRC (falls für AIRC lokale Verarbeitung in der Sphäre des Kunden konfiguriert ist)
 - DICOM Hub

Beschreibung der Verarbeitungsvorgänge:

- VV-01 Autorisierung von Benutzern
- VV-02 Steuerung des Datenflusses zwischen den Kundensystemen und den teamplay Anwendungen
- VV-03 teamplay-Benutzeroberfläche und Konfiguration der Institutionseinstellungen
- VV-04 teamplay MR Dashboard
- VV-05 teamplay CT Dashboard
- VV-06 teamplay X-ray Dashboard
- VV-07 teamplay Dose
- VV-08 teamplay Contrast
- VV-09 teamplay Usage
- VV-10 teamplay Protocols
- VV-11 teamplay Insights
- VV-12 teamplay Admin Center
- VV-13 AI-Rad Companion

Datenarten:

- Patientendaten
- Personal der Institution
- teamplay Nutzer
- Log Daten

Relevante Standorte:

Siemens Healthineers AG, Hartmannstraße 16, 91052 Erlangen

Prozesse:

teamplay wurde und wird nach einem für Siemens Healthineers einschlägigen PLM Prozess entwickelt und betrieben. Die entsprechenden Artefakte sind in den respektiven zentralen Systemen hinterlegt.

Applikationen:

- Appl-01: teamplay websites (Webapplikation mit Stand August 2025, teamplay.siemens-healthineers.com), weitere Navigation von der "home-" page aus. Alle Verarbeitungsvorgänge (VV) erfolgen mittels dieser Applikation.

IT-Infrastruktur:

- Client-01: Arbeitsplatzrechner, vorkonfigurierter SHS Windows Client der SHS Mitarbeitenden
- Speicher-01: Azure Blob Storage (von Microsoft Azure bereitgestellter Speicheraccount)
- DB-01: Azure DB Systeme (zahlreiche Tabellen von verschiedenen Datenbanksystemen (SQL-DB, non SQL-DB, Table Storage, je nach Anforderung der jeweiligen Verarbeitung)

- Serv-01: Azure Kubernetes Service (AKS), von Microsoft bereitgestellter Service. Alle dafür notwendigen Server werden von Microsoft verwaltet.
- Netz-01: Virtuelles Netz mit Web Application Firewall (WAF) und Loadbalancer. Die zugrundeliegenden Services werden von Microsoft bereitgestellt und von SHS verwaltet.
- Physische Infrastruktur:
 - Ort-01: Erlangen, Hartmannstr. 16/5.Stock

Externe Dritte:

- DL-01: Microsoft Ireland Operations Ltd., Zur-Verfügung-Stellung der Cloud Computing-Plattform Microsoft Azure an Standorten in Irland und Niederlande
- DL-02: Siemens Healthcare Private Limited, Indien
- DL-03: Siemens Healthcare s.r.o., Slowakei

Evaluierungsinformationen

Prüfverfahren, inklusive der Zertifizierung zugrundeliegender Kriterien (ggf. mit Versionsangabe):

datenschutz cert GmbH, „Kriterienkatalog zur Zertifizierung einer IT-gestützten Verarbeitung personenbezogener Daten gem. Art. 42 DSGVO („information privacy standard“), Version 1.0

Angewendete Evaluierungsmethoden

- Basisprüfung
- Prüfung (rechtl.)
- Prüfung (techn.)
- Auditierung/Inspektion

Zeitraum der Evaluierung

Insgesamt wurde die Evaluierung im Zeitraum 25.07.2025 bis 15.09.2025 (letzter Evaluierungstag = Abschluss der Evaluierung) durchgeführt.

Eingebundene Evaluatoren:

Dr. Irene Karper, Evaluatorin Recht, datenschutz cert GmbH
Matthias Mühlhause, Evaluator Technik, datenschutz cert GmbH

Prüfergebnis:

Der Zertifizierungsgegenstand erfüllt alle anwendbaren Kriterien des Zertifizierungsstandard „DSGVO – information privacy standard“ (Version 1.0).

Zertifizierungsinformationen

Evaluierungsart:

Erst-Zertifizierung

Angaben zu möglichen Überwachungstätigkeiten zur Aufrechterhaltung der Zertifizierung:

Letzter Tag der Evaluation: 15.09.2025

Überwachung 1: 14.09.2026

Überwachung 2: 14.09.2027

Zuständige Datenschutzaufsichtsbehörde:

Der Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen

Kurzgutachten

Es fand eine ausführliche Prüfung aller vorgelegter Dokumente statt.

Es fanden die folgenden Remote-Vorführungen mit Interviews für die Evaluatoren statt mit folgenden Schwerpunkten:

- teamplay Receiver Software
 - teamplay Plattform und darauf aufbauende Applikationen
 - AI Rad-Companion
- Während dieser Vorführungen wurden folgende Aspekte adressiert:
- Walkthrough durch alle Funktionen innerhalb und um die Applikationen herum
 - Fragestellungen speziell zu den TOMs
 - Authentifizierung und Autorisierung
 - Passwort Management
 - Netzwerksicherheit
 - Logging
 - Azure Management
 - Verschlüsselung

Am 09.09.2025 fand ein SiteVisit mit den Interviewpartnern statt am Standort Siemens Healthineers AG, Hartmannstraße 16, 91052 Erlangen. Das Evaluationsteam hat mit den Mitarbeitern der Siemens Healthineers Interviews geführt, die folgende Themen zum Gegenstand hatten:

- Zutrittskontrollen zu den Büroräumen von SHS am Standort Erlangen
- Administration von Azure
- Einsichtnahme/Review des einschlägigen ISO 27001 Reports
- Einsichtnahme/Review des einschlägigen Pentest-Reports basierend auf OWASP- und MITRE Framework.
- Review von Verträgen von allen Unterauftragnehmern, von Kundenverträgen und den Verträgen zur Auftragsverarbeitung
- Review von Vertraulichkeitsvereinbarungen der Mitarbeitenden
- Review von E-Learning-Inhalten zu Datenschutz und Informationssicherheit
- Review der Bearbeitung von Customer Requests in Ticketsystemen

Über eine öffentlich zugängliche Website kann sich jeder als Nutzer auf der teamplay-Plattform registrieren. Für die Registrierung und Authentifizierung wird der Authentifizierungsanbieter Autho (Okta) verwendet. Diese Funktionalitäten sind unabhängig vom Kunden (Verantwortlichen). Die Siemens Healthineers AG ist der Verantwortliche für die Registrierung und Authentifizierung von teamplay-Benutzern und zeigt den Benutzern bei der Registrierung die teamplay-Datenschutzerklärung (Privacy Notice) an. Da es sich hierbei nicht um eine Verarbeitung im Auftrag des Kunden handelt, ist dies nicht Bestandteil der Zertifizierung (Hinweis: die hierzu implementierten Datenschutz- und Sicherheitsmechanismen wurden jedoch in die Evaluation mit einbezogen, da sie zeigen, wie der Zugriff auf Kundendaten geschützt wird und wie die Transparenz und Informationspflichten in Abgrenzung zur Auftragsverarbeitung umgesetzt wurden).

Zusammenfassung der Ergebnisse

Die Dienste der cloudbasierten Plattform teamplay fördern den Datenschutz auf vielfältige Weise:

Die Datenschutzorganisation der Siemens Healthineers ist hervorragend in die Erstellung und Aktualisierung von Verfahrensverzeichnissen (HDP-Register) zu teamplay eingebunden, verschiedene Monitorings und Prüfungsmechanismen garantieren eine stetige Aktualität der Informationen.

Die für teamplay freiwillig durch Siemens Healthineers durchgeführten Data Protection Impact Assessments (DPIA) sind als vorbildlich zu bewerten.

Hervorzuheben sind Maßnahmen zur Datenminimierung sowie zur Pseudonymisierung und Anonymisierung von Patientendaten. Für jeden Dienst werden nur die DICOM-Studien hochgeladen, die für diese Funktionalität notwendig sind. Des Weiteren wird der Inhalt der DICOM-Studien minimiert. Um eine robuste Datenminimierung und Pseudonymisierung zu gewährleisten, werden die DICOM-Dateien mit Hilfe von "Allowlists" (Zulassungslisten) minimiert. Die Allowlists geben die DICOM-Attribute an, die entweder mit ihrem ursprünglichen Wert beibehalten, durch einen weniger genauen Wert oder durch ein Pseudonym ersetzt werden sollen. DICOM-Attribute, die nicht in der Allowlist aufgeführt sind, werden nicht hochgeladen. Die teamplay-Receiver-Software führt diese Datenminimierung in der Sphäre der Institution durch.

Kunden können zwischen verschiedenen „Privacy Levels“ (Datenschutzstufen) wählen, das Hochladen von personenbezogenen Daten über Personen, die an der Bildgebung beteiligt sind, z.B. Bediener des Gerätes oder anderes Personal der Institution, aktivieren und darüber hinaus applikationsspezifische Datenschutzoptionen auswählen.

Die Privacy Level definieren, in welchem Umfang die Patientendaten minimiert werden.

Das Privacy Level "Standard Privacy" lädt nur DICOM Studien mit pseudonymisierten Patienten-IDs hoch. Alle DICOM-Attribute, die direkt identifizierbare Informationen wie Name, Adresse oder Telefonnummer enthalten, werden nicht hochgeladen. Patientenmerkmale, die für Berechnungen notwendig sind, bleiben erhalten. Das Pseudonym wird durch ein Keyed Hash-Verfahren mit einem institutsspezifischen Schlüssel erzeugt.

Das Privacy Level „High Privacy“ liefert im Vergleich zu „Standard Privacy“ weniger Details bei den Patientenmerkmalen. Dieses Privacy Level bietet eine erhebliche Minimierung personenbezogener Daten. Einige Funktionen sind daher jedoch nur mit begrenzter Genauigkeit verfügbar.

Unter dem Privacy Level "Restrictive" werden weder Patienten-Identifikatoren noch ein Pseudonym des Patienten verwendet. Als Patientenmerkmale werden nur Geschlecht und Alterskategorie sowie der Untersuchungsmonat hochgeladen. Nicht alle Funktionen sind daher verfügbar. Bei Daten, die über den teamplay-DICOM-Hub hochgeladen werden, ist zu beachten, dass hier auch die Bilddaten hochgeladen werden. Bilddaten können u.U. die Identifizierung der jeweiligen Person ermöglichen, z.B. wenn es sich um einen Scan des Kopfes handelt.

Standardmäßig verarbeitet z. B. AI-Rad Companion nur pseudonymisierte Patientendaten in der Cloud. Eine erneute Identifizierung des Patienten innerhalb des teamplay Receivers ist notwendig, um die Ergebnisse der richtigen DICOM-Studie zuordnen zu können. In der Vorschau-Benutzeroberfläche in der Cloud werden Patientenkennungen für teamplay-Benutzer angezeigt, die sich im Krankenhausnetzwerk befinden. Diese Daten werden von Systemen im Krankenhaus gesammelt und in der Benutzeroberfläche zusammengeführt, Patientenidentifikatoren werden nicht in der Cloud verarbeitet. Diese Re-Identifizierung stellt sicher, dass Patienten für die klinische Entscheidungsfindung eindeutig identifiziert werden können.

Die Funktionalität der Anwendungen wird auf der Grundlage von Kundenfeedback und von gesetzlichen Anforderungen (z.B. Dosismanagement) kontinuierlich verbessert. Weitere technische Daten, die in den DICOM-Studien enthalten sind, könnten hochgeladen werden, um die Anwendungen zu verbessern. Wenn für eine Funktionalität ein DICOM-Attribut mit personenbezogenen Daten erforderlich ist, wird im Rahmen der vorhandenen Privacy Level eine neue Option entwickelt und als neue Funktion angeboten, um diesen Upload zu ermöglichen.

Anwender werden durch transparente Informationen und Beschreibungen in die Lage versetzt, Beschäftigten- und Patientendaten datenschutzkonform und datensparend zu verarbeiten.

Verbesserungspotentiale ergeben sich lediglich im Hinblick auf die textliche Korrektur einiger vorgelegter Dokumente.

Abweichungen zu den Kriterien wurden nicht festgestellt.

Anlage 2

Ausschlüsse Evaluierungsinformationen

Ausschlüsse von Kriterien gemäß Statement of Applicability (SOA)

Gemäß Statement of Applicability (SOA) ausgeschlossene Elemente:

- P.1.2 Rechtsgrundlage Vertrag
- P.1.3 Rechtsgrundlage berechtigtes Interesse
- P.1.4 Rechtsgrundlage Einwilligung
- P.1.5 Rechtsgrundlage rechtliche Verpflichtung
- P.1.6 Rechtsgrundlage lebenswichtige Interessen
- P.1.7 Rechtsgrundlage öffentliches Interesse
- P.1.8 Verarbeitung bei besonderen Kategorien personenbezogener Daten
- P.1.9 Verarbeitung bei strafrechtlichen Verurteilungen und Straftaten
- P.6.5 Datenschutz-Folgenabschätzung
- P.7.2 Vertreter innerhalb der EU
- P.8.9 Automatisierte Entscheidungen/Profiling

Ausschlüsse von dem Zertifizierungsgegenstand

Nicht Teil des Zertifizierungsgegenstandes sind folgende Bestandteile:

- Die Verarbeitung personenbezogener Daten durch die Siemens Healthineers AG in der Rolle als verantwortliche Stelle wurde nicht zertifiziert.
- Die Nutzung von teamplay durch Gesundheitseinrichtungen außerhalb Deutschlands ist nicht Bestandteil des Zertifizierungsgegenstands.
- Alle Funktionen, die zur Verwaltung des Geschäftsverhältnisses mit dem Kunden erforderlich sind, werden von SHS in der Rolle des Verantwortlichen verarbeitet. Daher sind die Registrierung der Institutionen, die Institutionsinformation, das Document Center, und die Lizenzen nicht Bestandteil der Zertifizierung.
- Die Registrierung neuer teamplay-Benutzer, die Authentifizierung von teamplay-Benutzern, die Abmeldung und die Integration von Siemens Healthineers ID-Benutzern über Federation sowie die Datenverarbeitung als Identity Provider wird von der Siemens Healthineers AG in der Rolle des Verantwortlichen verarbeitet und ist nicht Gegenstand der Zertifizierung. (Hinweis: die hierzu implementierten Sicherheitsmechanismen wurden jedoch in die Evaluation mit einbezogen, da sie zeigen, wie der Zugriff auf Kundendaten geschützt wird.)
- Ebenfalls nicht Bestandteil des Zertifizierungsgegenstands ist die Authentifizierung über Identity Provider der Kunden.
- Kunden können weitere Dienste, die auf der teamplay-Plattform laufen, lizenzieren. Diese Dienste sind nicht Bestandteil der Zertifizierung.
- Die Datenverarbeitung und Anzeige von Daten aus anderen Anwendungen innerhalb von teamplay Insights, etwa mit ActExcell ist nicht Teil der Zertifizierung, da dies ein weiterer, größtenteils von teamplay unabhängiger Dienst ist, der optional erworben werden kann.

- Die teamplay Plattform und die teamplay Dienste haben Schnittstellen zu anderen Anwendungen und Diensten, die nicht Teil der Zertifizierung sind.
- Optional konfigurierte Anwendungen sind nicht Teil der Zertifizierung, da SHS darauf keinen Einfluss hat.
- Über das Admin Center steht eine dedizierte Softwarekomponente zur Verfügung, die auf dem Gerät installiert werden kann, um asymmetrische Schlüssel zu generieren und die Anforderung und den Download von Zertifikaten zu verwalten. Diese Software ist nicht Teil des Zertifizierungsgegenstands, da es sich nur um eine optionale Unterstützung für Siemens Healthineers-Geräte handelt.
- teamplay Audit-Logs, insbesondere die Benutzerverwaltung (inkl. Benutzer-Logins) enthalten per Definition den teamplay-Benutzer, der die Aktion initiiert. Für die Erstellung von teamplay Audit-Logs zur Authentifizierung fungiert die Siemens Healthineers AG als Verantwortlicher, weshalb die betreffenden Verarbeitungsvorgänge nicht Bestandteil der Zertifizierung sind.
- Dedizierte Software, Betriebssysteme (z.B. Windows), Backend-Hardware sind nicht Teil der Zertifizierung, da es sich nicht um eine Hauptleistung von teamplay handelt bzw. die Betriebssysteme von Drittunternehmen zur Verfügung gestellt werden.
- Die Siemens Healthineers AG oder ihre verbundenen Unternehmen können im Zusammenhang mit den teamplay-Diensten und dem teamplay Receiver Remote-Support-Dienste anbieten. Diese Zusatzleistung ist optional und deshalb nicht Bestandteil der Zertifizierung.
- Der Siemens Healthineers Digital Marketplace ist nicht Teil der Zertifizierung da er von Siemens Healthineers AG in der Rolle des Verantwortlichen betrieben wird.