

Vertragliche Bedingungen zur Auftragsverarbeitung („AV-Vertrag nach Art. 28 DSGVO“)

(Version: 01.02.2025)

Dieser AV-Vertrag ergänzt und konkretisiert die datenschutzrechtlichen Verpflichtungen des zwischen den Vertragspartnern abgeschlossenen Hauptvertrages als Anlage. Der AV-Vertrag findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiter von Siemens Healthineers oder durch Siemens Healthineers beauftragte Dritte personenbezogenen Daten des Kunden verarbeiten. Die Regelungen in diesem AV-Vertrag entsprechend Art. 28 DSGVO dienen ausschließlich der Umsetzung der datenschutzrechtlichen Anforderungen der DSGVO für die Auftragsverarbeitung und haben nicht die Übernahme einer Einstandspflicht oder sonstigen Gewährleistung für andere oder einer verschuldensunabhängigen Haftung von Siemens Healthineers - gleich aus welchem Rechtsgrund - zum Gegenstand.

0. Interpretation

- 0.1. Soweit in diesem AV-Vertrag Begriffe verwendet werden, die in der DSGVO definiert sind, haben diese Begriffe die gleiche Bedeutung wie in der DSGVO.
- 0.2. Dieser AV-Vertrag ist im Lichte der Bestimmungen der DSGVO zu lesen und auszulegen.
- 0.3. Dieser AV-Vertrag darf nicht in einer Weise ausgelegt werden, die den in der DSGVO vorgesehenen Rechten und Pflichten zuwiderläuft, oder in einer Weise, die die Grundrechte oder -freiheiten der betroffenen Datensubjekte beeinträchtigt.

1. Gegenstand, Art, Zweck, Zweckbindung und Dauer der Verarbeitung

- 1.1. Dieser AV-Vertrag ergänzt den zwischen den Vertragspartnern abgeschlossenen Hauptvertrag. Er bezieht sich auf die Verarbeitung personenbezogener Daten durch Siemens Healthineers als „Auftragsverarbeiter“ im Auftrag des Kunden (dem „Verantwortlichen“) im Rahmen des Hauptvertrags und regelt die datenschutzrechtlichen Pflichten der Vertragspartner. Die konkrete Beschreibung von Gegenstand, Art, Zweck und Dauer der Verarbeitung personenbezogener Daten durch Siemens Healthineers für den Kunden ist in den bestehenden und zukünftigen Hauptverträgen enthalten.
- 1.2. Art und Zweck der Verarbeitung: Siemens Healthineers verarbeitet personenbezogene Daten, soweit dies erforderlich ist, um die im Hauptvertrag beschriebenen und vereinbarten Leistungen zu erbringen. Für andere Zwecke darf Siemens Healthineers die personenbezogenen Daten nicht verarbeiten.
- 1.3. Siemens Healthineers und der Kunde sind für die Einhaltung der jeweils für sie geltenden datenschutzrechtlichen Bestimmungen selbst verantwortlich. Der Kunde darf Siemens Healthineers keine personenbezogenen Daten zur Verfügung stellen, für welche die Rechtmäßigkeit einer Offenlegung an Siemens Healthineers nicht gegeben ist und für welche der Kunde keine gesetzliche Legitimation zur Verarbeitung hat.
- 1.4. Die Dauer der Auftragsverarbeitung entspricht der Laufzeit des Hauptvertrags.

2. Art der personenbezogenen Daten und Kategorien von Betroffenen

In Abhängigkeit der Festlegungen des Hauptvertrages sind die Kategorien der betroffenen Personen, deren personenbezogene Daten verarbeitet werden, insbesondere Mitarbeiter, Patienten, Kontaktpersonen des Kunden und Vertragspartner des Kunden. In Abhängigkeit der Festlegungen des Hauptvertrages sind insbesondere folgende Arten von personenbezogenen Daten Bestandteil der Verarbeitung: Kontaktinformationen, Identifizierungsmerkmale, Standortdaten, Finanzinformationen und sensitive Daten wie Gesundheitsdaten, Genetische Daten, Biometrische Daten.

3. Weisungen

- 3.1. Siemens Healthineers verarbeitet personenbezogene Daten nur auf der Grundlage dokumentierter Weisungen des Kunden. Dieser AV-Vertrag und der Hauptvertrag sind die vollständigen und abschließend dokumentierten Weisungen des Kunden an Siemens Healthineers zur Verarbeitung personenbezogener Daten.

- 3.2. Zusätzliche oder abweichende Weisungen sind vom Kunden schriftlich zu erteilen und nur verbindlich nach schriftlicher Bestätigung von Siemens Healthineers. Siemens Healthineers wird den Kunden informieren, wenn nach Auffassung von Siemens Healthineers eine Weisung des Kunden gegen die DSGVO oder die für Siemens Healthineers als Auftragsverarbeiter geltenden Datenschutzbestimmungen verstößt. Siemens Healthineers ist nicht verpflichtet, eine umfassende rechtliche Prüfung durchzuführen oder gesetzlich verbotene Anweisungen zu befolgen.
- 3.3. Der Kunde trägt alle Mehrkosten, die Siemens Healthineers durch zusätzliche oder abweichende Weisungen entstehen, es sei denn, die Weisung ist zur Einhaltung der für Siemens Healthineers geltenden gesetzlichen Vorschriften erforderlich.

4. Vertraulichkeit

Siemens Healthineers gewährt Mitarbeitern nur in dem Umfang Zugang zu den personenbezogenen Daten, soweit dies für die Durchführung, Verwaltung und Abwicklung des Hauptvertrages unbedingt erforderlich ist. Zur Wahrung der Vertraulichkeit gem. Art. 28 Abs. 3 lit. b DSGVO und von Geheimnissen (z.B. i.S.v. § 203 StGB) gewährleistet Siemens Healthineers, dass nur befugte Personen, die sich zur über das Arbeitsverhältnis hinaus bestehenden Verschwiegenheit verpflichtet haben oder einer entsprechenden gesetzlichen Verschwiegenheitspflicht unterliegen, mit der Verarbeitung personenbezogener Daten betraut werden. Dem eingesetzten Personal ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen.

5. Sicherheit der Verarbeitung

- 5.1. Siemens Healthineers trifft alle nach Artikel 32 DSGVO erforderlichen Maßnahmen.
- 5.2. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen und insbesondere der Risiken, die mit der Verarbeitung verbunden sind, insbesondere durch unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugtem Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet werden, wird Siemens Healthineers technische und organisatorische Maßnahmen gemäß Anlage TOM ergreifen.
- 5.3. Der Kunde und Siemens Healthineers sind sich darüber einig, dass die Umsetzung der in Anlage TOM beschriebenen technischen und organisatorischen Maßnahmen ein angemessenes Sicherheitsniveau im Einklang mit den Anforderungen der DSGVO gewährleistet und ausreichende Garantien für den Schutz der Rechte des Betroffenen bietet.
- 5.4. Die in Anlage TOM beschriebenen technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung und können von Siemens Healthineers gegebenenfalls angepasst werden, solange eine solche Anpassung nicht zu einem niedrigeren Schutzniveau als in Anlage TOM beschrieben führt.

6. Weitere Auftragsverarbeiter

- 6.1. Ohne vorherige Genehmigung des Kunden wird Siemens Healthineers keine Verarbeitungstätigkeiten an weitere Auftragsverarbeiter vergeben. Wenn Siemens Healthineers Verarbeitungstätigkeiten mit Genehmigung des Kunden an weitere Auftragsverarbeiter vergibt, dürfen die weiteren Auftragsverarbeiter personenbezogene Daten nur zur Durchführung der Tätigkeiten verarbeiten, für die diese personenbezogenen Daten Siemens Healthineers zur Verfügung gestellt wurden. Es ist weiteren Auftragsverarbeitern untersagt personenbezogene Daten für andere Zwecke zu verarbeiten. Die Beauftragung eines weiteren Auftragsverarbeiters erfolgt durch einen Vertrag, der dem weiteren Auftragsverarbeiter im Wesentlichen die gleichen Datenschutzpflichten auferlegt, wie sie Siemens Healthineers nach diesem AV-Vertrag auferlegt sind, insbesondere soll der Vertrag ausreichende Sicherheiten für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen in der Weise bieten, dass die Verarbeitung den Anforderungen der DSGVO entspricht, der Schutz der Rechte der betroffenen Datensubjekte gewährleistet ist und Datenübermittlungen sowie die entsprechenden hinreichenden Garantien dokumentiert sind. Auf Verlangen des Kunden stellt Siemens Healthineers dem Kunden eine Kopie eines solchen Unterauftragsverarbeitungsvertrags und etwaige spätere Änderungen zur Verfügung. Soweit dies zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten, erforderlich ist, kann Siemens Healthineers den Text der Vereinbarung vor der Weitergabe der Kopie unkenntlich machen.
- 6.2. Eine Liste der weiteren Auftragsverarbeitern ist verfügbar unter <https://fleet.siemens-healthineers.com/welcome>. Siemens Healthineers hat die generelle Genehmigung des Kunden für die Beauftragung der auf der Liste aufgeführten Unternehmen als weitere Auftragsverarbeiter. Siemens Healthineers ist dafür verantwortlich von den weiteren Auftragsverarbeitern die entsprechenden Informationen einzuholen und die Liste aktuell zu halten. Der Kunde wird sich zum Erhalt dieser Information sowie für beabsichtigte Änderungen der Liste in Bezug auf die Hinzuziehung oder die Ersetzung von weiteren Auftragsverarbeitern auf der bereitgestellten Internetseite von Siemens Healthineers registrieren. Die Hinzuziehung oder Ersetzung eines weiteren Auftragsverarbeiters gilt als genehmigt, wenn Siemens Healthineers den Kunden hierüber vorher informiert und wenn der Kunde innerhalb von 30 Tagen nach dieser Information keine Einwände gegenüber Siemens Healthineers in schriftlicher oder elektronischer Form erhebt.
- 6.3. Widerspricht der Kunde, so hat er Siemens Healthineers die Gründe für den Widerspruch mitzuteilen.
- 6.4. Siemens Healthineers kann nach eigenem Ermessen aufgrund eines Widerspruchs
 - a. anstelle des abgelehnten weiteren Auftragsverarbeiters einen anderen weiteren Auftragsverarbeiter vorschlagen; oder
 - b. zur Beseitigung des Widerspruchs des Kunden Maßnahmen ergreifen, welche die Bedenken des Kunden ausräumen.
- 6.5. Stehen die Möglichkeiten unter (4) a. und b. vernünftigerweise nicht zur Verfügung oder ist der Widerspruch des Kunden nicht anderweitig beseitigt worden, kann Siemens Healthineers den Hauptvertrag ganz oder teilweise und ohne Einhaltung einer Frist kündigen, z. B. wenn der Widerspruch des Kunden dazu führt, dass Siemens Healthineers die Erfüllung der nach dem Hauptvertrag geschuldeten Pflichten nicht unerheblich erschwert oder unmöglich wird.
- 6.6. Ab der geplanten Hinzuziehung oder Ersetzung eines widersprochenen weiteren Auftragsverarbeiters sind etwaige Vereinbarungen über Reaktionszeiten oder Verfügbarkeiten suspendiert und es entfallen insofern sämtliche Ansprüche

wegen Schadensersatz statt der Leistung, wegen Verzögerungsschäden und auf etwaig vereinbarte Vertragsstrafen gegen Siemens Healthineers. Bei Teilkündigung der der Leistungsverpflichtungen von Siemens Healthineers bestimmt sich die Vergütung für die nicht von der Teilkündigung erfassten Leistungen nach den für diese Leistungen bei Siemens Healthineers geltenden üblichen listenmäßigen Preisen.

- 6.7. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet Siemens Healthineers gegenüber dem Kunden für die Einhaltung der Pflichten des Weiteren Auftragsverarbeiters. Siemens Healthineers haftet jedoch nicht für Schäden und Ansprüche, die sich aus zusätzlichen oder abweichenden Weisungen des Kunden im Sinne von § 3 Abs. 2 dieses AV-Vertrags ergeben.
 - 6.8. Werden weitere Auftragsverarbeiter in einem Drittland (außerhalb der EU/EWR) hinzugezogen, sind insbesondere die Vorgaben gemäß der Art. 44 ff. DSGVO zu beachten. Der Kunde stimmt zu, dass in Fällen, in denen ein weiterer Auftragsverarbeiter gemäß diesem § 6 mit der Durchführung bestimmter Verarbeitungstätigkeiten für den Kunden beauftragt wird und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne der Artikel 44 ff. DSGVO beinhalten, die Einhaltung der Artikel 44 ff. DSGVO entweder durch die Verwendung von Standarddatenschutzklauseln, die von der Kommission gemäß Artikel 46 Absatz 2 DSGVO erlassen wurden, sichergestellt werden kann, sofern die Bedingungen für die Verwendung dieser Standarddatenschutzklauseln erfüllt sind, oder durch die Verwendung anderer geeigneter Garantien gemäß Artikel 46 DSGVO.
- ## 7. Unterstützung
- 7.1. Unter Berücksichtigung der im Hauptvertrag und in diesem AV-Vertrag beschriebenen Art der Verarbeitung wird Siemens Healthineers den Kunden auf Verlangen und auf Kosten des Kunden und soweit dies möglich ist, durch geeignete technische und organisatorische Maßnahmen dabei unterstützen, der Verpflichtung des Kunden zur Beantwortung von Anträgen auf Wahrnehmung der in Art. 12 bis 23 DSGVO genannten Rechte der betroffenen Person nachzukommen.
 - 7.2. Siemens Healthineers wird den Kunden unverzüglich über Anträge von betroffenen Personen auf Wahrnehmung der in Art. 12 bis 23 DSGVO genannten Rechte, insbesondere hinsichtlich des Rechts auf Auskunft, Berichtigung, Löschung („Recht auf Vergessenwerden“), Verarbeitungseinschränkung, Datenübertragbarkeit sowie des Widerspruchsrechts und des Rechts auf nichtautomatisierte Entscheidungen im Einzelfall einschließlich Profiling, informieren.
 - 7.3. Unter Berücksichtigung der im Hauptvertrag und in diesem AV-Vertrag beschriebenen Art der Verarbeitung sowie der Siemens Healthineers zur Verfügung stehenden Informationen unterstützt Siemens Healthineers den Kunden auf Kosten des Kunden bei der Einhaltung seiner Verpflichtungen gemäß
 - a. Art. 32 DSGVO (Verarbeitungssicherheit);
 - b. Art. 33 DSGVO (Benachrichtigung bei Verletzung personenbezogener Daten an die Aufsichtsbehörde): Im Falle einer Verletzung des Schutzes personenbezogener Daten in Bezug auf personenbezogene Daten, die von Siemens Healthineers verarbeitet werden, benachrichtigt Siemens Healthineers den Kunden unverzüglich, nachdem Siemens Healthineers von der Verletzung Kenntnis erlangt hat. Diese Benachrichtigung muss mindestens Folgendes enthalten:
 - (i) eine Beschreibung der Art der Verletzung (einschließlich, soweit möglich, der Kategorien und der ungefähren Anzahl der betroffenen Personen und Datensätze);
 - (ii) die Angaben einer Kontaktstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

(iii) die wahrscheinlichen Folgen der Verletzung und die getroffenen oder geplanten Maßnahmen zur Behebung der Verletzung, einschließlich der Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Ist es nicht möglich, alle diese Informationen gleichzeitig bereitzustellen, so enthält die erste Benachrichtigung die zu diesem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, unverzüglich nachgereicht;

c. Art. 34 DSGVO (Benachrichtigung bei Verletzung personenbezogener Daten an die betroffene Person);

d. Art. 35 DSGVO (Benachrichtigung über die Folgenabschätzung der Auswirkungen auf den Datenschutz); und

e. Art. 36 DSGVO (Beurteilung der Datensicherheit).

7.4. In dem Fall, dass der Kunde Unterstützung benötigt, sollte der Kunde das Büro des Datenschutzbeauftragten von Siemens Healthineers unter der folgenden E-Mailadresse kontaktieren: dataprivacy.func@siemens-healthineers.com.

8. Löschung

Nach Wahl des Kunden sind nach Abschluss der Erbringung von Verarbeitungsleistungen alle personenbezogenen Daten entweder zu löschen oder zurückzugeben. Siemens Healthineers wird hiermit angewiesen nach Abschluss der Erbringung der Verarbeitungsleistungen die vom Kunden erhaltenen personenbezogenen Daten zu löschen, es sei denn, dass das Recht der Union oder des Mitgliedstaates die Speicherung der personenbezogenen Daten vorschreibt. Solange die personenbezogenen Daten nicht gelöscht sind, muss Siemens Healthineers für die Einhaltung der Bedingungen dieses AV-Vertrages sorgen.

9. Informations- und Prüfungsrechte

9.1. Hinsichtlich der Verarbeitung im Rahmen des Hauptvertrages wird Siemens Healthineers dem Kunden auf sein schriftliches Verlangen hin alle Informationen zur Verfügung stellen, die erforderlich sind, um die Einhaltung der Verpflichtungen nach Art. 28 DSGVO nachzuweisen.

9.2. Ferner wird Siemens Healthineers Überprüfungen, einschließlich Inspektionen („Audits“), in Bezug auf die Verarbeitung im Rahmen des Hauptvertrags ermöglichen und sich daran beteiligen. Audits können auch von einem unabhängigen, vom Kunden beauftragten externen Auditor durchgeführt werden, sofern der externe Auditor für Siemens Healthineers akzeptabel ist und einer Pflicht zur Geheimhaltung unterliegt, die nicht weniger restriktiv ist als die im Rahmen des Hauptvertrags für den Kunden geltende. Der Kunde wird ein Audit mit angemessener Frist ankündigen. Vor der Durchführung eines Audits vereinbaren die Vertragspartner den Umfang, den Zeitpunkt und die Dauer des Audits. Der Kunde hat Siemens Healthineers die Siemens Healthineers im Zusammenhang mit dem Audit anfallenden Leistungen zu den jeweils aktuellen Siemens Healthineers-Servicetarifen zu vergüten, welche dem Kunden auf Verlangen zur Verfügung gestellt werden.

9.3. Der Kunde hat Siemens Healthineers unverzüglich schriftlich einen Bericht zu erstatten, der eine vertrauliche Zusammenfassung von Umfang und Ergebnissen des Audits enthält. Siemens Healthineers ist berechtigt, den Bericht für eigene Zwecke zu verwenden.

Anlage TOM:

Technische und Organisatorische Maßnahmen („TOM“) Siemens Healthineers

1. Pseudonymisierung und Verschlüsselung personenbezogener Daten

Siemens Healthineers trennt personenbezogene Daten von den verarbeiteten Daten, so dass eine Verknüpfung der verarbeiteten Daten mit einer identifizierten oder identifizierbaren Person ohne zusätzliche Informationen, die gesondert und sicher aufbewahrt werden, nicht möglich ist. Siemens Healthineers verschlüsselt personenbezogene Daten mit symmetrischen oder asymmetrischen Schlüsseln.

2. Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste

Siemens Healthineers sichert die Vertraulichkeit und Integrität mit folgenden Maßnahmen:

Zutrittskontrolle:

Siemens Healthineers schützt seine Gebäude durch angemessene Zutrittskontrollsysteme, basierend auf einer Sicherheitseinstufung der Gebäude und einem entsprechend definiertem Zutrittsberechtigungskonzept. Alle Gebäude sind durch Zutrittskontrollmaßnahmen unter Verwendung eines Kartenlesersystems gesichert. Je nach Sicherheitskategorie werden Grundstücke, Gebäude oder einzelne Bereiche durch zusätzliche Maßnahmen gesichert. Dazu gehören spezielle Zutrittsprofile, Biometrie, Pin- Pads, DES-Dongles, Vereinzelungsschleusen, Videoüberwachung und Wachpersonal. Zutrittsrechte für berechtigte Personen werden gemäß festgelegten Kriterien individuell erteilt. Dies gilt auch hinsichtlich externer Personen.

Systemzugangskontrolle:

Zugang zu Datenverarbeitungssystemen erhalten nur authentifizierte Benutzer aufgrund eines rollenbezogenen Berechtigungskonzepts unter Verwendung von folgenden Maßnahmen: Datenverschlüsselung, individualisierte Passwortvergabe (mindestens 8 Zeichen, regelmäßig automatisch ablaufend), Mitarbeiterausweise mit PKI-Verschlüsselung, passwortgeschützte Bildschirmschoner bei Inaktivität, Intrusion-Detection-Systeme und Intrusion-Prevention-Systeme, regelmäßig aktualisierte Antiviren- und Spyware-Filter im Netzwerk und auf den einzelnen PCs und mobilen Endgeräten.

Datenzugriffskontrolle:

Zugriff auf personenbezogene Daten wird auf der Grundlage eines rollenbezogenen Berechtigungskonzepts gewährt. Es ist ein Benutzerverwaltungssystem eingerichtet, welches den Zu- und Abgang von Nutzern mit ihren jeweiligen Berechtigungen abbildet und zentral im Netzwerk zum Abruf durch anfragende Datenverarbeitungssysteme zur Verfügung steht. Ferner werden unberechtigte Zugriffe auf personenbezogene Daten durch Datenverschlüsselung verhindert.

Datenübertragungskontrolle:

Siemens Healthineers sichert die elektronischen Kommunikationswege durch Einrichtung geschlossener Netzwerke und Verfahren zur Datenverschlüsselung ab. Sofern ein physischer Datenträgertransport erfolgt, existieren überprüfbare Transportprozesse, welche den unbefugten Datenzugriff oder den logischen Verlust verhindern. Datenträger werden datenschutzgerecht entsorgt.

2.1 Siemens Healthineers stellt die ständige Verfügbarkeit und Belastbarkeit der Systeme und Dienste mit folgenden Maßnahmen sicher:

Die Verfügbarkeit und Belastbarkeit der Systeme und Dienste sichert Siemens Healthineers durch die Isolierung kritischer IT- und Netzwerkkomponenten, durch die Bereitstellung

geeigneter Backup- und Redundanzsysteme, durch den Einsatz von Stromredundanzsystemen sowie durch regelmäßige Tests der Systeme und Dienste. Test- und Live-Systeme sind vollständig getrennt.

3. Verfügbarkeit der und Zugang zu personenbezogenen Daten bei Zwischenfall

Siemens Healthineers stellt die Verfügbarkeit der und den Zugang zu personenbezogenen Daten bei einem physischen oder technischen Zwischenfall mit folgenden Maßnahmen wieder her:

Siemens Healthineers speichert personenbezogene Daten in RAID-Systemen und integriert redundante Systeme entsprechend der Sicherheitskennzeichnung. Zur Sicherung der Stromversorgung in den Rechenzentren setzt Siemens Healthineers Systeme für eine unterbrechungsfreie Stromversorgung ein (z. B. USVs, Batterien, Generatoren). Datenbanken oder Rechenzentren werden an verschiedenen physikalischen Orten gespiegelt. Ein umfassender schriftlicher Notfallplan ist vorhanden. Notfallprozesse und -systeme werden regelmäßig überprüft.

4. Kontrollverfahren zur Gewährleistung der Sicherheit der Verarbeitung

Siemens Healthineers unterhält ein Kontrollverfahren auf der Grundlage eines risikomanagementbasierten Ansatzes unter Berücksichtigung der IT-Grundschutz-Kataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI) sowie der ISO/IEC 27001 zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. Damit wird der Schutz der relevanten Informationen, Anwendungen (einschließlich Qualitäts- und Sicherheits-Testmethoden), Betriebsumgebungen (z.B. durch Netzwerküberwachung gegen schädliche Einwirkungen) sowie der technischen Umsetzung von Schutzkonzepten (z. B. mittels Schwachstellenanalysen) gewährleistet. Durch das systematische Erfassen und Beseitigen von Schwachstellen werden damit die Schutzmaßnahmen kontinuierlich hinterfragt und verbessert.

5. Personelle Maßnahmen

Siemens Healthineers erteilt schriftliche Arbeitsanweisungen und schult regelmäßig Personal mit Zugang zu personenbezogenen Daten, um sicherzustellen, dass personenbezogene Daten nur in Übereinstimmung mit dem Gesetz, diesem AV-Vertrag und den dazugehörigen Weisungen des für die Verarbeitung Verantwortlichen einschließlich der beschriebenen technischen und organisatorischen Maßnahmen verarbeitet werden.