Cloud-Lösungen für das Monitoring von Umgebungsbedingungen in GxP-Anwendungsbereichen

Sinnvoller Ansatz oder bester Weg, sich die Finger zu verbrennen?

Dr. Philipp Osl • ELPRO-BUCHS AG, Buchs SG (Schweiz)
Bob Lucchesi • USDM Life Sciences, Santa Barbara (USA)

Korrespondenz: Dr. Philipp Osl, Head of Product Management, ELPRO-BUCHS AG, Langäulistrasse 45, 9470 Buchs SG (Schweiz); **e-mail**: philipp.osl@elpro.com

PEER REVIEW

Zusammenfassung

Um den GxP-Anforderungen zu entsprechen, müssen entlang der Herstellungs- und Lieferkette von pharmazeutischen Produkten die Umgebungsbedingungen überwacht und dokumentiert werden. Dazu werden vermehrt Cloud-Lösungen eingesetzt. Die Frage, ob dies ein sinnvoller Ansatz ist, wird kontrovers diskutiert. Der Beitrag beschreibt unterschiedliche Cloud-Modelle und damit verbundene Nutzen sowie Risiken und liefert eine Checkliste für den Einsatz von Cloud-basierten Monitoring-Lösungen in GxP-Anwendungsbereichen.

Key Words

- Monitoring
- Temperaturüberwachung
- GxP
- Cloud
- Checkliste

1. Einleitung

In den letzten Jahren ist die Akzeptanz für Cloud Computing und Cloud Hosting auch für Geschäftsanwendungen in unterschiedlichsten Branchen markant gestiegen. Dies ist auf offensichtliche Vorteile wie Skalierbarkeit (sowohl hinsichtlich der Datenverarbeitung als auch -speicherung), integrierte Backup- und Wiederherstellungsfunktionen, reduzierter Wartungsaufwand, einfacher Zugriff insbesondere bei geografisch verteilten Teams sowie in vielen Fällen auch auf Kosteneinsparungen durch niedrigere IT-Investitionen und benötigtes In-House-Know-how zurückzuführen. Trotz der zunehmenden Verbreitung bestehen weiterhin auch eine Reihe von Bedenken, z. B. bzgl. Lock-In-Effekten und daraus resultierenden Abhängigkeiten, Sicherheitsaspekten oder generell eines Kontrollverlusts.

Aufgrund der zahlreichen oben erwähnten Vorteile überrascht es trotz der ebenfalls vorhandenen Unsicherheiten und Bedenken kaum, dass auch Unternehmen, welche GxP-Anforderungen erfüllen müssen, mehr und mehr Interesse zeigen, Anwendungen in der Cloud zu betreiben. Als Konsequenz daraus bieten immer mehr Anbieter von GxP-relevanten Anwendungen Cloud-basierte Lösungen an. Und dennoch wird die Frage, ob Cloud-Anwendungen den GxP-Anforderungen entsprechen (können) und worauf geachtet werden muss, um die Konformität sicherzustellen, weiterhin z. T. kontrovers diskutiert. Dieser Beitrag versucht, Antworten auf diese Fragen zu geben mit einem speziellen Fokus auf Cloud-basierten Anwendungen zur Überwachung der Umgebungsbedingungen in der Pharma-, Life-Science-, Biotech- und Healthcare-Industrie.

1.1 Adressaten und Ziele des Beitrags

Alle Unternehmen, die GxP-Vorschriften einhalten müssen, erhalten eine ausführliche Diskussion über Vor- und Nachteile von Cloud-Lösungen sowie Vorschläge zu Maßnahmen, um die Konformität sicherzustellen.

Unternehmen, die konkret über Cloud-basierte GxP-Anwendungen nachdenken, erhalten eine Checkliste zu Dokumenten und Informationen, die sie entweder selbst erstellen und festlegen müssen, oder vom Anbieter der Cloud-Lösung einfordern sollten.

2. Über „die Cloud"

2.1 Was ist die Cloud?

Vor der Diskussion spezifischer Punkte zu Cloud-basierten Monitoring-Lösungen im GxP-Umfeld sollen kurz die verschiedenen Modelle von Cloud-Diensten erläutert

TechnoPharm 9, Nr. 3, 144–153 (2019)

werden. Normalerweise werden 3 Cloud-Modelle unterschieden, die sich im Umfang der ausgelagerten Teile vom traditionellen lokalen Hosting (on-premises) unterscheiden (Abb. 1, [1]).

„Infrastructure as a Service" (*IaaS*) ist jenes Cloud-Modell, bei dem der Kunde den größten Teil selbst verantwortet. In diesem Modell betreibt der Kunde auf zumeist virtualisierten Servern des Cloud-Anbieters seine eigenen Betriebssysteme, eigene Middleware und Laufzeit-Umgebung, auf der seine Applikationen mit den zugehörigen Daten laufen. IaaS ist v. a. für große Organisationen von Vorteil, die vollständige Kontrolle über ihre Anwendungen und Software-Infrastrukturen haben möchten, die Hardware jedoch in einem Rechenzentrum eines spezialisierten Anbieters betreiben wollen oder nur das kaufen möchten, was tatsächlich genutzt wird (z. B. zur Abdeckung von Bedarfsspitzen hinsichtlich Rechenleistung oder Speicherplatz). Dieses Modell könnte sich etwa für ein Life-Science-Unternehmen anbieten, welches weniger kritische Anwendungen auf einem IaaS-Server betreiben möchte, um so von den Vorteilen des Outsourcings zu profitieren, gleichzeitig aber die Kontrolle über die Anwendung zu behalten.

„Platform as a Service" (*PaaS*) überträgt mehr Verantwortung an den Cloud-Anbieter, indem dieser nicht nur die (virtualisierten) Server betreibt, sondern sich auch für Betriebssysteme, Middleware und Laufzeit-Umgebung verantwortlich zeichnet. PaaS bietet Unternehmen, die ihre eigenen Anwendungen in einer „schlüsselfertigen Umgebung" ausführen möchten, hohe Geschwindigkeit und Flexibilität für den gesamten Prozess. Ein Beispiel für dieses Modell könnte ein Pharmaunternehmen sein, das seine Office-Anwendungen auf einem PaaS-Angebot eines großen Cloud-Anbieters wie Amazon Web Services oder Microsoft Azure betreibt.

„Software as a Service" (*SaaS*), häufig auch als „Cloud Application Services" bezeichnet, ist der größte Cloud-Markt. SaaS stellt (Geschäfts-) Anwendungen bereit, die typischerweise direkt über den Webbrowser aufgerufen werden können. Somit sind weder Download noch Installation der Software durch den Kunden nötig, sondern er kann die durch die Lösung bereitgestellten Funktionalitäten direkt nutzen.

Neben den verschiedenen oben beschriebenen Cloud-Modellen, die sich durch die ausgelagerten Komponenten unterscheiden, können auch verschiedene Modelle für die Bereitstellung dieser ausgelagerten Cloud-Ressourcen unterschieden werden:

- *Public Cloud* bezeichnet ein Cloud-Modell, bei dem IT-Services über das Internet bereitgestellt

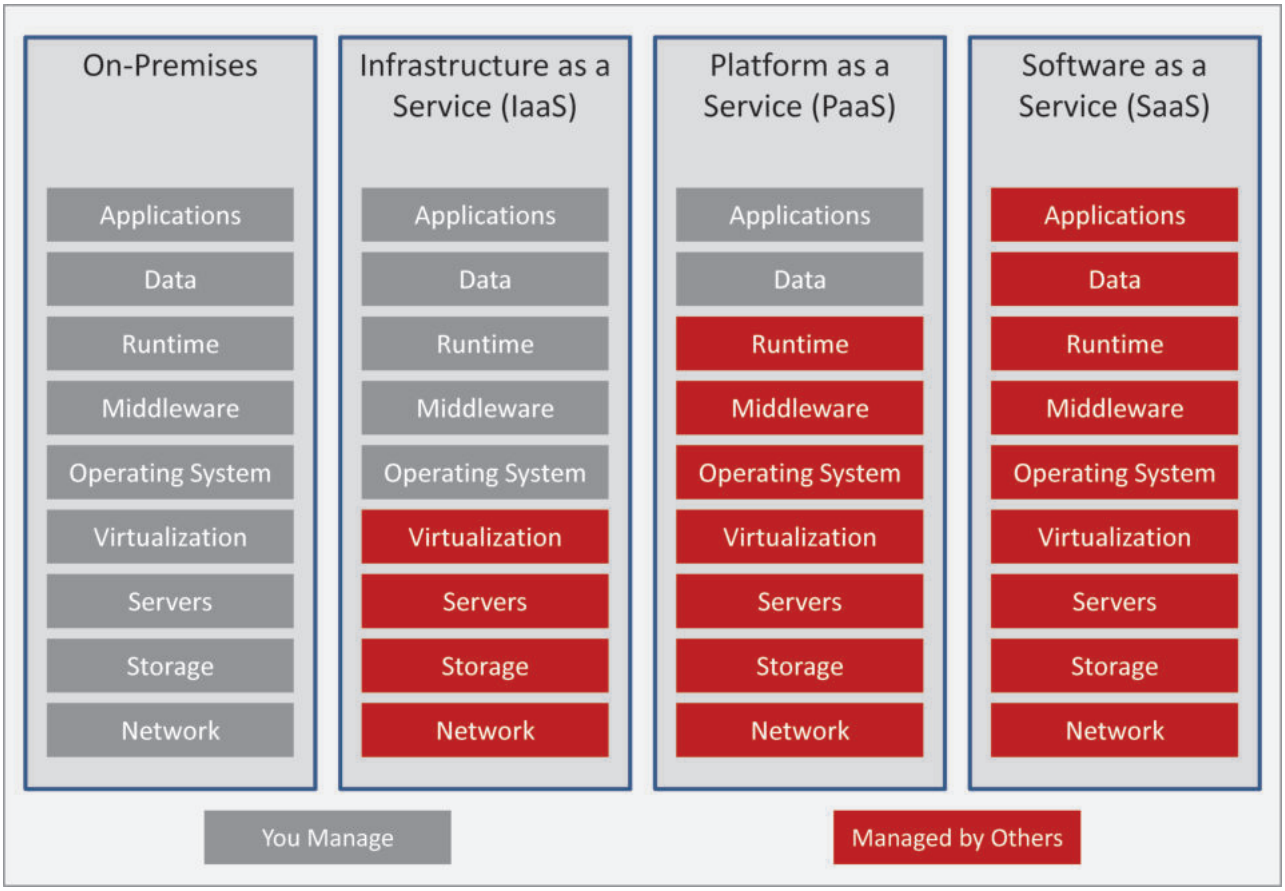


Abbildung 1: Unterschiedliche Cloud-Modelle (Quelle aller Abbildungen: ELPRO-BUCHS AG).

werden und von mehreren Mandanten aus dem gesamten Netzwerk gemeinsam genutzt werden. Der Cloud-Anbieter ist für die Entwicklung, Verwaltung und Verteilung des gemeinsam genutzten Pools von Ressourcen verantwortlich. Eine Unterart der Public Cloud ist die sog. *Community Cloud*, die ebenfalls von mehreren Organisationen gemeinsam genutzt wird. Allerdings ist diese nicht öffentlich für jeden zugänglich, sondern wird von einem definierten Nutzerkreis mit gleichen Anforderungen gemeinsam genutzt. Die gemeinsamen Interessen können z. B. in der Einhaltung von offiziellen Compliance-Vorgaben wie Audit-Vorschriften liegen. Oder sie können mit Anforderungen an die Performance zu tun haben, also z. B. für das Hosten von Anwendungen, die schnelle Antwortzeiten erfordern [2].

- *Private Cloud* bezeichnet Cloud-Lösungen, die von einer einzelnen Organisation verwendet werden. Die Ressourcen sind isoliert und werden nicht mit anderen Kunden geteilt. Verglichen mit der Public Cloud ist die Private Cloud wesentlich teurer, da die Ressourcen für jeden neuen Kunden separat bereitgestellt werden müssen.
- *Hybrid Cloud* bezeichnet eine Mischung aus öffentlicher und privater Cloud. Die Ressourcen werden normalerweise als integrierte Infrastrukturumgebung orchestriert, die von Apps und Daten-Workloads den geschäftlichen und technischen Richtlinien des Unternehmens entsprechend gemeinsam genutzt werden können. Hybrid Cloud bietet „das Beste aus beiden Welten", jedoch zum Preis gesteigerter Komplexität.

Cloud Computing ist ein wichtiger Trend und die Umsätze explodieren. Bemerkenswert dabei ist, dass Finanzdienstleister/Banken/Versicherungen, die industrielle Fertigung und Telekommunikationsdienste zu den Branchen mit den meisten Cloud-Anwendungen pro Geschäftsfunktion gehören [3]. Dies zeigt deutlich, dass heute auch (oder sogar überwiegend) Branchen mit hohen Anforderungen an Compliance und Sicherheit Cloud-Computing-Dienste verwenden.

2.2 Das richtige Cloud-Setup für eine GxP-konforme Anwendung

Nachfolgend wird die Eignung verschiedener Cloud-Setup-Optionen anhand der Kern-Anforderungen einer Monitoring-Lösung beurteilt.

Eine Monitoring-Lösung einschließlich der Datenbank muss aufgrund der Qualitäts-Relevanz *validiert* werden. Die Validierung computergestützter Systeme (Computerized System Validation, CSV) ist der dokumentierte Prozess, um sicherzustellen, dass ein System genau das auf konsistente und reproduzierbare Weise tut, was es tun soll. Im Wesentlichen bedeutet dies, dass Anforderungen dokumentiert, Validierungs- und Testpläne erstellt, Risiken in einer schriftlichen Risikobeurteilung bewertet, die Funktionalitäten getestet und gemäß Testplan dokumentiert werden müssen und schließlich ein Validierungsbericht erstellt werden muss, der alle Validierungsbemühungen zusammenfasst. Eine IaaS- oder PaaS-Lösung könnte darum der richtige Ansatz sein, wenn der Anwender den Cloud-Infrastrukturanbieter auditiert und die Softwareinstallation und -wartung sowie die Qualifizierung der gesamten Lösung selbst vornehmen kann. Für Anwender, die sich nicht damit befassen möchten bzw. keine erfahrene IT-Abteilung als Unterstützung zur Hand haben, lohnt sich ein Blick in Richtung SaaS-Lösung, die den zusätzlichen Vorteil bietet, nur einen Cloud-Lösungsanbieter zu haben, anstatt sich mit dem Anbieter der Monitoring-Software einerseits und dem Anbieter der Cloud-Infrastruktur andererseits auseinandersetzen zu müssen.

Für die Entscheidung zwischen Public, Private oder Hybrid Cloud sind v. a. die *Kosten* ausschlaggebend. Entscheidend hierfür ist, auf wie viele Nutzer einzelne Kostenblöcke verteilt werden können.

- Unabhängig vom Cloud-Modell entstehen je Organisation individuelle Kosten für die genutzte Mess-Hardware wie Datenlogger und Fühler.
- Bei einer Public Cloud können sämtliche Kosten im Zusammenhang mit der Monitoring-Software auf die verschiedenen Nutzer aufgeteilt werden. Üblicherweise verrechnet der SaaS-Anbieter diese zu einem Preis je genutztem Messpunkt. Somit übernimmt der SaaS-Anbieter das Risiko einer Unterdeckung im Falle weniger Nutzer, profitiert aber andererseits finanziell, wenn viele Messpunkte auf der gemeinsam genutzten Softwareinstanz betrieben werden. Der Anwender profitiert preislich von der Verteilung der Kosten auf mehrere Schultern und einer niedrigen finanziellen Einstiegshürde, da keine Investitionen in Form zu tragender Fixkosten für den Betrieb der Monitoring-Software entstehen.
- Bei einer Private Cloud werden die Cloud-Ressourcen nicht mit anderen Nutzern geteilt. Entsprechend entstehen Fixkosten durch die bereitzustellende isolierte Infrastruktur (z. B. Server, Lizenzen für Betriebssystem und Applikationen), die der SaaS-Anbieter i. d. R. auch als Fixposten an den Kunden verrechnen wird. Werden die Infrastrukturkosten als Fixkosten verrechnet, reduzieren sich die variablen Softwarekosten je Messpunkt um diesen Anteil.
- Für die Bewertung des Hybrid-Cloud-Modells gehen die Autoren davon aus, dass dieses v. a. im Falle kundenindividueller Verteilungen zwischen öffentlichen und privaten Cloud-Ressourcen zur Anwendung kommt. In diesem Szenario ist davon auszugehen, dass kundenspezifische Entwicklungskosten sowie Kosten für die Validierung der verteilten Architektur direkt vom Anwender zu tragen sein werden. Infrastruktur-

TechnoPharm 9, Nr. 3, 144–153 (2019)

Pharmawasser

Kosten für den privaten Teil der hybriden Lösung werden ebenfalls dem Kunden direkt verrechnet, während die notwendige Infrastruktur für den öffentlichen Teil wiederum durch mehrere Nutzer getragen werden kann und somit in einem variablen Preis für die Monitoring-Applikation je Messpunkt enthalten sein könnte.

Abbildung 2 zeigt die verschiedenen Kostenblöcke der unterschiedlichen Cloud-Modelle als schematische Darstellung. Daraus wird offensichtlich, dass vor allem für kleine Installationen die Public Cloud eine kostenmäßig attraktive Lösung aufgrund des Wegfalls von vom Kunden direkt zu tragenden Fixkostenblöcken ist. Bei größeren Installationen mit mehreren hundert oder tausend Messpunkten relativiert sich dieser Kostenvorteil.

In einer GxP-Umgebung müssen *Daten unveränderlich* sein. Das Hauptanliegen sind wiederum die Datenintegrität (Sicherstellung, dass die Daten über den gesamten Lebenszyklus hinweg zuordenbar, lesbar, zeitnah, original, genau, vollständig, konsistent, dauerhaft und verfügbar sind [4, 5]) und in weiterer Folge die Patientensicherheit. Auf eine Cloud-basierte Überwachungslösung übersetzt bedeutet dies:

- Unabhängig vom gewählten Cloud-Setup wird eine Anwendung mit sauber getrennten Funktionsschichten auf einer sicheren Infrastruktur benötigt, in der Daten sicher sind und nicht manipuliert werden können. Nach Einschätzung der Autoren ist kaum eine IT-Abteilung eines Nutzers von Monitoring-Lösungen in der Lage, ein Rechenzentrum professioneller und sicherer zu führen als die global agierenden Cloud-Anbieter wie z. B. Amazon Web Services, Microsoft Azure oder Google Cloud Platform. Im Übrigen sind sich alle diese Provider der besonderen Anforderungen von GxP-Anwendungen bewusst und bieten umfangreiches Dokumentationsmaterial für Kunden und Lösungsanbieter an, die entsprechende Anwendungen in ihrer Infrastruktur betreiben möchten.
- Darüber hinaus sind die Autoren der Meinung, dass die technischen Risiken bzgl. Datenintegrität am besten vom Anbieter der Monitoring-Lösung eingeschätzt werden können, der über das größte Wissen bzgl. allen miteinander verbundenen Komponenten des Systems verfügt. Unter der Annahme, dass alle Seiten ihr Expertenwissen verantwortungsvoll einbringen, erscheint daher weiterhin ein Public-Cloud-SaaS-Angebot als eine naheliegende Wahl für Installationen jeder Größe, insbesondere für kleinere Installationen aufgrund der Kostenvorteile, während ein Private-Cloud-SaaS-Angebot eine charmante Alternative für größere Installationen sein kann. Letzteres Modell könnte – im Vergleich zum Public-Cloud-SaaS-Angebot – mehr Raum für das Management von Software-Updates gemäß den individuellen

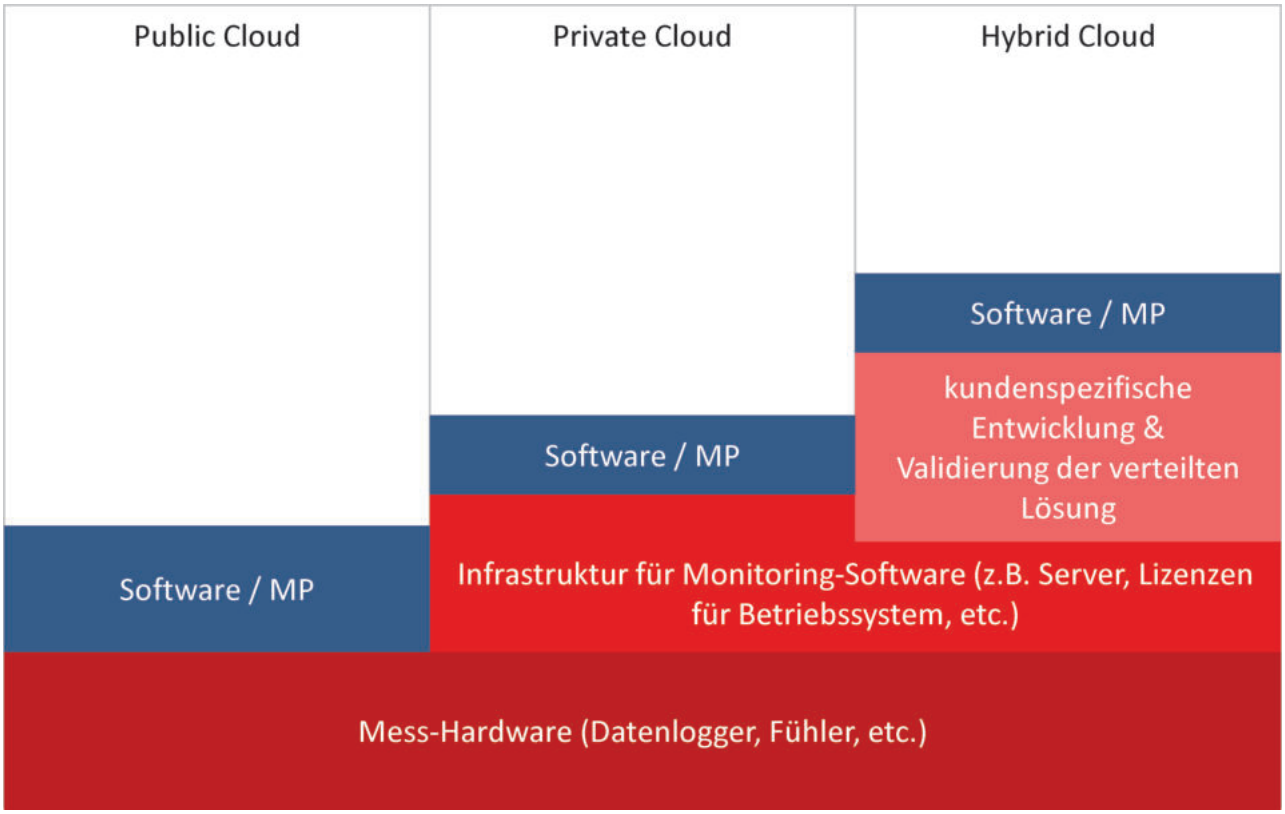


Abbildung 2: Kostenblöcke in verschiedenen Cloud-Modellen (schematische Darstellung).

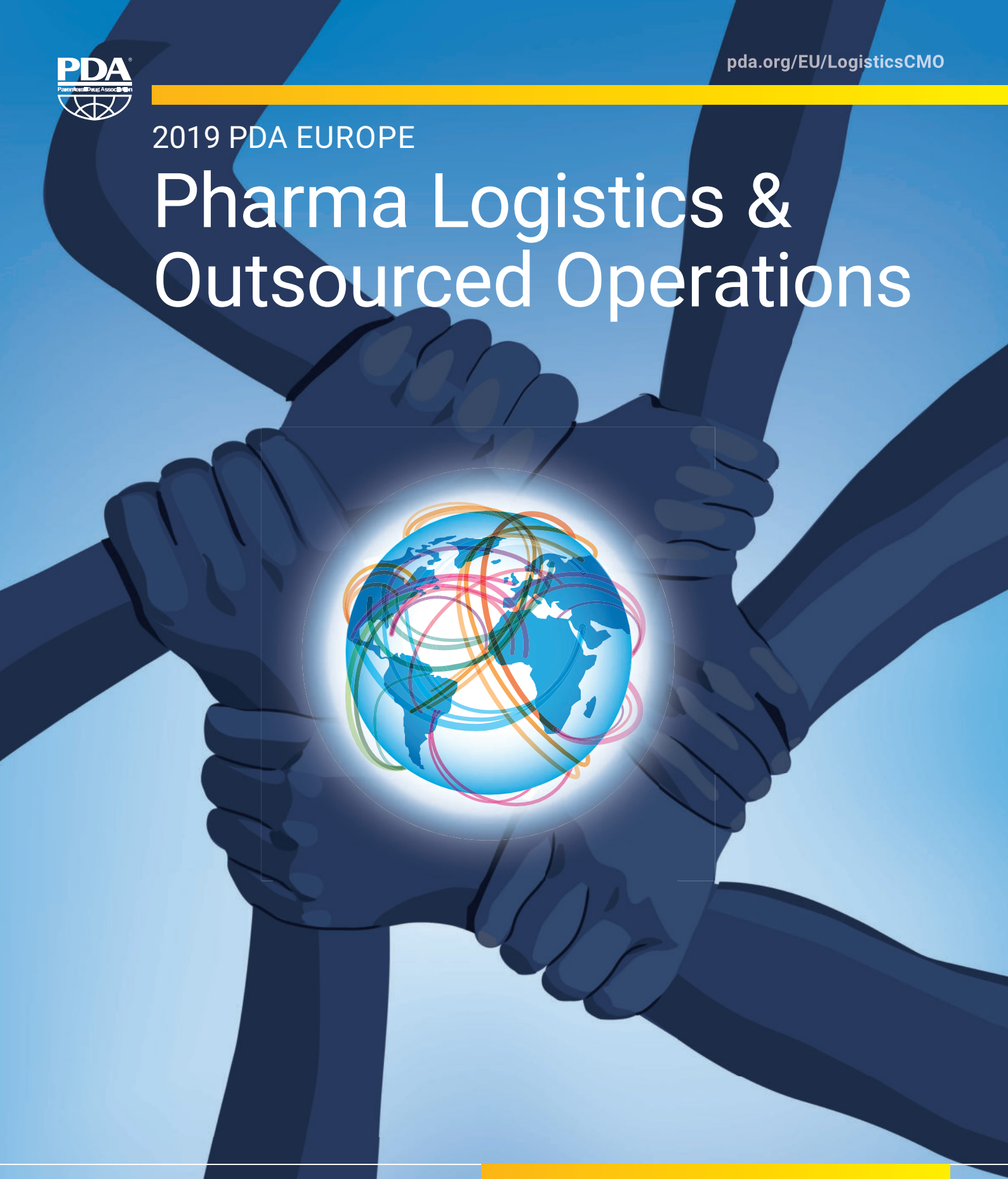
TechnoPharm 9, Nr. 3, 144–153 (2019)

PDA
Parenteral Drug Association

pda.org/EU/LogisticsCMO

2019 PDA EUROPE

Pharma Logistics & Outsourced Operations



12-13 NOVEMBER 2019
LISBON, PORTUGAL
EXHIBITION: 12-13 NOVEMBER
IG MEETING: 14 NOVEMBER

REGISTER BEFORE 15 SEPTEMBER AND SAVE UP TO €200!

CONNECTING PEOPLE SCIENCE AND REGULATION®

Qualifizierungsanforderungen des Nutzers bieten, da die Überwachungslösung nur von einem Unternehmen genutzt und nicht zwischen verschiedenen Mandanten geteilt wird.

Zwischenfazit: Angesichts der oben ausgeführten Argumentation verwundert es kaum, dass immer mehr Anbieter Monitoring-Lösungen für GxP-kritische Anwendungen als *SaaS in einer Public Cloud* anbieten. Diese Wahl bietet maximale Qualität (minimale Risiken) zu gleichzeitig minimalen Kosten. Viele Anbieter werden Single-Tenant *SaaS in einer Privaten Cloud* alternativ zu deutlich höheren Kosten anbieten. Die folgenden Kapitel konzentrieren sich auf diese beiden Modelle für GxP-konforme Cloud-basierte Überwachungslösungen.

3. Risiken und Maßnahmen zur Risikominderung bei Cloud-basierten GxP-konformen Überwachungslösungen

In diesem Kapitel werden die Risiken von Cloud-basierten Monitoring-Lösungen, die entweder als Public Cloud SaaS (gemeinsame Instanz für mehrere Mandanten) oder als Private Cloud SaaS (separate Instanzen jeweils ausschließlich für ein Unternehmen) angeboten werden, sowie sinnvolle Risikominderungsstrategien diskutiert. Es ist ratsam, sich diese Ansätze zur Reduktion des Risikos vom Anbieter in entsprechenden Vereinbarungen garantieren zu lassen.

- Bei SaaS-Angeboten definiert der Lieferant den *physischen Ort der Datenspeicherung*. Daten können auf verschiedenen Kontinenten, in unterschiedlichen Regionen und Ländern gespeichert werden, die abweichende Gesetze und Vorschriften in Bezug auf Datenschutz und Privatsphäre haben. So können personenbezogene Daten (wie Namen, Adressen, Telefonnummern oder Kreditkarten) z. B. der europäischen Datenschutz-Grundverordnung (DSGV/GDPR) oder den US-HIPAA-Vorschriften bzgl. „Privacy of Personal Identifiable Information" unterliegen. Der Dienstleister muss daher sicherstellen (und im Service Level Agreement bestätigen), dass
  - geeignete Sicherheitsmaßnahmen zum Schutz der Daten (vor unbefugtem Zugriff) getroffen werden,
  - geeignete Sicherheitsmaßnahmen zur Sicherung der Daten (vor Löschung und Verlust) getroffen werden,
  - der Datenschutz gewährleistet ist (und die Lösung die Anforderungen der DSGVO und anderer Datenschutzbestimmungen erfüllt).
- Jede GxP-konforme Lösung muss *validiert* werden. Für ein SaaS-Angebot, das entweder als Public- oder Private-Cloud-Lösung angeboten wird, bedeutet dies insbesondere, dass der Dienstleister Folgendes erfüllen muss:
  - Bereitstellung eines Nachweises, der bestätigt, dass alle Komponenten der Überwachungslösung nach den Standards von GAMP5 entwickelt wurden, inklusive Validierungsplan, Risikoanalyse und Validierungsbericht aller Hard- und Software-Komponenten
  - Bereitstellung der Installation Qualification (IQ) der Software auf der Cloud
  - Bereitstellung von Tools, die eine effiziente Qualifizierung durch den Kunden ermöglichen und insbesondere das kundenindividuelle Zusammenspiel von Mess-Hardware und Software berücksichtigen: IQ (= „welche Mess-Hardware wurde installiert") und OQ (Operational Qualification = „arbeitet die Lösung aus Mess-Hardware und -Software wie geplant, z. B. alarmiert sie wie vorgesehen").
- Einer der größten Vorteile von SaaS ist, dass sich der Anbieter um *Patches und Updates* kümmert. Wie kann die GxP-Konformität des Kunden sichergestellt werden? Wenn ein Auditor die Validierungs- und Qualifizierungsmaßnahmen der Überwachungslösung sehen möchte, die Software aber ständig aktualisiert wird – wie soll dies zusammengehen? Hier sehen die Autoren die größten Unterschiede zwischen einer gemeinsamen Instanz in der Public Cloud und einer Single-Tenant-Instanz, die als Private Cloud SaaS angeboten wird. In jedem Fall muss der Anbieter Folgendes bereitstellen:
  - Definierte Regeln und Prozesse bzgl. Benachrichtigungen, Dokumentation und Qualifizierung als Teil des Service Level Agreements (für Private-Cloud-SaaS-Angebote kann es Raum zur individuellen Gestaltung dieser Richtlinien geben, um sie an die Bedürfnisse des Kunden hinsichtlich Vorankündigungsfristen oder Test- und Qualifizierungsmöglichkeiten vorgängig zum Update anzupassen)
  - Bereitstellung von Benachrichtigungen und Dokumentationen zu Änderungen am System (Patches sind i. d. R. geringfügige (minor) Änderungen und müssen zumindest dokumentiert werden; Upgrades müssen im Voraus angekündigt und als „minor" oder „major" eingestuft und entsprechend dokumentiert werden). In jedem Dokument sollte klar angegeben werden, ob kundenseitige Maßnahmen empfohlen sind.
  - Alle oben genannten Informationen müssen für den Kunden jederzeit verfügbar und zugänglich sein, insbesondere auch während eines Audits. Idealerweise stehen alle Dokumente direkt als Teil des Cloud-Services bereit.
- Der Kunde muss dem Dienstleister vertrauen können, dass die *Da-*

TechnoPharm 9, Nr. 3, 144–153 (2019)

tenintegrität immer gesichert ist. Der Dienstleister muss
  - sicherstellen, dass Rohdaten (z. B. Messwerte) unter keinen Umständen verändert werden können,
  - einen Audit Trail implementieren, der alle Ereignisse und Änderungen dokumentiert und angemessene Audit-Trail-Reviews unterstützt,
  - im Service Level Agreement bestätigen, dass die Sicherstellung der Unverfälschtheit, Konsistenz und Vollständigkeit der Daten über den gesamten Lebenszyklus hinweg gewährleistet ist.
- Ein großes Anliegen ist *Business Continuity* – insbesondere in einem SaaS-Setup, bei dem der Kunde keinerlei Kontrolle über den Betrieb der Lösung hat. Der Anbieter muss
  - Leistung und Verfügbarkeit der Lösung definieren und im Service Level Agreement garantieren,
  - sicherstellen, dass das System und alle Daten regelmäßig gesichert werden und die Wiederherstellung eines Backups regelmäßig (testhalber) durchgeführt und dokumentiert wird,
  - Verfügbarkeit und Leistung der Lösung überwachen und entsprechende Berichte den Kunden bereitstellen.
- Die *Archivierung* ist in den GxP-Vorschriften nicht einheitlich geregelt und unterscheidet sich je nach Nutzungsfall [6], wie z. B. Produktion, Forschung und Zulassung, Blutprodukte, Medizingeräte usw. Hinzu kommt, dass jede Firma nach eigener risikobasierter Beurteilung die vorgeschriebene Archivierungsdauer verlängern kann. Somit ergeben sich Anforderungen an Archivierungszeiträume von 10 Jahren, manchmal auch von 15 Jahren oder länger. Es ist einfach, Dateien und elektronische Daten über viele Jahre hinweg zu speichern, aber ein großes Problem ist die Verfügbarkeit von Software zur Analyse derselben. Viele Menschen glauben, dass archivierte Daten für immer genau so verfügbar sein sollten, wie sie erzeugt wurden. Demgegenüber definiert TechTarget [7, übersetzt] Datenarchivierung wie folgt:
- *„Datenarchivierung ist der Prozess der Übertragung von Daten, die nicht mehr aktiv genutzt werden,*

auf ein separates Speichermedium zur langfristigen Aufbewahrung. Archivdaten bestehen aus älteren Daten, die für das Unternehmen noch wichtig sind und für zukünftige Referenzen benötigt werden können, sowie aus Daten, die für die Einhaltung gesetzlicher Vorschriften aufbewahrt werden müssen."

- Somit ergeben sich abweichende Anforderungen an „Archivdaten" gegenüber „Prozessdaten":
  - *Prozessdaten* sind „frische Daten", die verwendet werden, um geschäftsrelevante Entscheidungen zu treffen (z. B. ein Produkt betreffend, Mittlere-kinetische-Temperatur(MKT)-Berechnung für eine Stabilitäts-Studie). Der Zeitraum, in dem Daten als Prozessdaten verfügbar sein müssen, ist abhängig von der Applikation. Für diese Dauer muss der Anbieter Folgendes sicherstellen:
    - Prozessdaten sind elektronisch verfügbar und visualisierbar (z. B. Zoom, Überlagerungen),
    - Prozessdaten können einfach statistisch ausgewertet werden (z. B. Berechnung der MKT),
    - Es muss möglich sein, Kommentare im System zu ergänzen und Berichte zu generieren (z. B. Freigabe-Entscheidungen),
    - Es muss möglich sein, die Daten zu exportieren (z. B. zur Verwendung in einem übergeordneten Batch Management System).
  - Werden die Daten in den Geschäftsprozessen nicht mehr benötigt, können sie als *Archivdaten* ihren Speicherort und ihre Form ändern. Der Anbieter muss sicherstellen, dass – je nach Anwendungsfall (vgl. [6]) – die Archivdaten mindestens 10 Jahre lang verfügbar sind und die folgenden Anforderungen erfüllen:
    - klar gekennzeichnet/beschriftet (z. B. Monatsbericht pro Sensor)
    - verfügbar als „menschenlesbare" Aufzeichnung (z. B. PDF/A-Bericht)
    - gespeichert in einem sicheren Archiv (z. B. auf einem Laufwerk, das regelmäßig an einem anderen physischen Ort gesichert wird).
- Durch die Auswahl eines GxP-Monitoring-Anbieters unterwirft sich der Kunde einem *Lock-in* mit diesem Dienstleister. Wie kann si-

Checkliste für den Einsatz von Cloud-basierten Monitoring-Lösungen in GxP-Anwendungsbereichen

- Ist die Lösung als „Software-as-a-Service" (SaaS) verfügbar?
- Ist die Lösung als Private-Cloud- oder Public-Cloud-Angebot verfügbar?
  - <100 Messpunkte: Public Cloud verfügbar?
  - >100 Messpunkte: Private Cloud verfügbar?
- Führt der Anbieter eine umfassende Validierung seiner computergestützten Systeme durch (CSV) und liefert er einen dokumentierten Nachweis über die Validierungsmaßnahmen?
- Garantiert der Anbieter die Unveränderbarkeit der Messwerte?
- Gibt es einen Audit Trail, in dem jeder Login(-Versuch), jedes Vorkommnis und jede Aktion mit Zeitstempel und Benutzer dokumentiert sind?
- Sind die Daten vor unautorisiertem Zugriff geschützt?
- Werden regelmäßig Backups der Daten erstellt und diese an einem sicheren Ort gespeichert?
- Wird die Wiederherstellung von Daten regelmäßig getestet und dokumentiert?
- Ist der Datenschutz gewährleistet? Erfüllt die Lösung die relevanten Anforderungen aus der DSGVO und anderen Datenschutzrichtlinien?
- Ist ein Nachweis für die Lösung verfügbar, welcher die Entwicklung entsprechend den GAMP5-Standards bestätigt?
- Sind Validierungsplan, Risikoanalyse und Validierungsbericht verfügbar?
- Stehen Qualifizierungs-Templates für die IQ und OQ zur Verfügung?
- Sind Benachrichtigungsprozesse, Dokumentation und Qualifikation klar geregelt?
- Gibt es klare Regelungen zu Benachrichtigungen inklusive Vorlaufzeiten sowie zur Dokumentation von Änderungen am System (Patches und Updates)?
- Sind Leistung und Verfügbarkeit der Lösung klar definiert?
- Werden Berichte zu Leistung und Verfügbarkeit des Systems den Kunden regelmäßig zur Verfügung gestellt?
- Sind Prozessdaten verfügbar, solange sie in den Geschäftsprozessen benötigt werden?
- Können Daten für mindestens 10 Jahre in einem menschenlesbaren Format archiviert werden?
- Bleibt der Kunde Eigentümer der Daten?
- Akzeptiert der Anbieter Vor-Ort-Audits durch Kunden?
- Sind alle oben genannten Punkte im Service Level Agreement festgeschrieben?

TechnoPharm 9, Nr. 3, 144–153 (2019)

chergestellt werden, dass die Daten weiterhin verfügbar sind, falls der Anbieter aus dem Geschäft ausscheidet oder die Lösung nicht mehr angeboten wird?
  - Es ist darauf zu achten, eine Kopie der Daten (z. B. monatliche Sensorberichte) in einem für Menschen lesbaren Format (z. B. PDF/A) bei sich aufzubewahren (z. B. automatisierte monatliche E-Mail an den internen Mail-Account).
  - Im Service Level Agreement muss festgelegt sein, dass der Kunde Eigentümer der Daten bleibt und dass die Daten vor Beendigung des Angebots zum Herunterladen zur Verfügung stehen.
  - Das Service Level Agreement muss eine sinnvolle Kündigungs- respektive Vorankündigungsfrist vor Beendigung des Angebots festlegen.

Neben einem Service Level Agreement, das alle oben genannten Punkte festhält, muss ein Anbieter Cloud-basierter Monitoring-Lösungen für GxP-Anwendungen auch *Vor-Ort-Audits durch Kunden* akzeptieren. Im Rahmen dieser Audits muss den Kunden Folgendes möglich sein:

- Zugriff auf die detaillierte GAMP5-Dokumentation zur Überprüfung des Nachweises des Anbieters
- Überprüfung relevanter Account-Management-Richtlinien, z. B. für Accounts auf den Cloud-Servern (Wer hat von Seiten des Anbieters Zugriff auf die Cloud-Infrastruktur? Wie werden diese Personen angeleitet/geschult?)
- Überprüfung der Richtlinien für den Zugriff auf Kundenkonten (Wer hat von Seiten des Anbieters Zugriff auf welche Daten des Kunden? Wie werden diese Personen angeleitet/geschult?)
- Überprüfung von Verträgen/Service Level Agreements mit Drittanbietern von Cloud-Infrastrukturen (wie z. B. Amazon Web Services, Microsoft Azure usw.), sofern genutzt
- Überprüfung von Berichten bzgl. „Service-Organization-Control (SOC) 2“ für das verwendete Rechenzentrum oder den verwendeten Cloud-Infrastrukturanbieter (häufig wird dies als ausreichender Nachweis der Qualifikation des Infrastrukturanbieters akzeptiert, da die SOC-2-Berichte detaillierte Informationen zur Konformität von Rechenzentren liefern). „Service Organization Control 2“ ist ein Standard, gemäß dem Service-Organisationen Berichte zu Sicherheit, Verfügbarkeit, Integrität der Verarbeitung, Vertraulichkeit und Datenschutz erstellen. Der Standard wurde nach den AICPA Trust Services Principles and Criteria erstellt. [8]

4. Zusammenfassung

Bei richtiger Umsetzung und sorgfältiger Auswahl des Anbieters bieten Cloud-basierte Monitoring-Lösungen Vorteile wie Kosteneffizienz, Skalierbarkeit, Komfort (keine Softwarewartung), hochprofessionelle Backup- und Wiederherstellungsstrategien usw. auch für Unternehmen, die GxP-Vorschriften einhalten müssen. Hinsichtlich des Validierungs- und Qualifizierungsbedarfs gelten für Cloud-Dienste die gleichen Anforderungen wie für selbst betriebene Systeme. Dies bedeutet, dass die Dokumentation höchste Priorität hat und die bei Cloud-basierten Lösungen geteilte Zuständigkeit hierfür zwischen Anbieter und Nutzer im Service Level Agreement klar definiert werden muss. Neben der zentralen Dokumentation zur Systemvalidierung müssen im Rahmen des Service Level Agreements auch kritische Prozesse wie z. B. das Änderungsmanagement (Updates und Patches) oder die Datensicherung und -wiederherstellung zur Gewährleistung der Business Continuity sowie die Langzeitarchivierung definiert werden. Darüber hinaus sollte der Dienstleister Audits durch Kunden akzeptieren, bei denen diese Zugang zu detaillierteren Dokumentationen erhalten.

Klare, unmissverständliche Regelungen von Zuständigkeiten einerseits und die durch den Anbieter bereitgestellten (zwar umfangreichen aber dennoch handhabbaren) Dokumente andererseits geben den Kunden nicht nur die notwendige Unterstützung und Sicherheit bzgl. ihrer GxP-Konformität, sondern sie tragen auch dazu bei, eine starke Partnerschaft zwischen dem Anbieter der Cloud-basierten Überwachungslösung und dem Kunden zu etablieren. Und dieses Verständnis einer Partnerschaft ist wahrscheinlich der wichtigste Erfolgsfaktor, um das erforderliche Maß an Konformität und „Audit Fitness“ für den Kunden zu erreichen, der immer für die Sicherheit der Patienten verantwortlich bleibt.

Literatur

[1] SaaS vs PaaS vs IaaS: What's The Difference and How To Choose, Stephen Watts, 22. Sep. 2017, *https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/*

[2] Community-Cloud, Margaret Rouse, last updated Feb. 2012, *https://www.computerweekly.com/de/definition/Community-Cloud*

[3] Differences in Cloud Adoption Across Global Industries, by TATA consultancy services, undatiert, *https://sites.tcs.com/cloudstudy/differences-in-cloud-adoption-across-global-industries*

[4] Ensuring Data Integrity Through ALCOA, Grant South, 29. Apr. 2016, *https://www.pharmout.net/data-integrity-alcoa/*

[5] CSV Considerations Around Data Integrity, Kelly Jordan, 03. March 2016, *https://www.propharmagroup.com/blog/csv-considerations-around-data-integrity/*

[6] Archivierung elektronischer Daten im GxP-Umfeld, Dr. Bernhard Appel et al., *https://www.apv-mainz.de/fileadmin/dateiablage/apv-mainz/Publikationen/1207-1215_Hornberger.pdf*

[7] Data Archiving, Definition on TechTarget, last updated Nov. 2018, *https://searchdatabackup.techtarget.com/definition/data-archiving*

[8] SOC 2 (Service Organization Control 2), Margaret Rouse, last updated Apr. 2012, *https://www.searchsecurity.de/definition/SOC-2-Service-Organization-Control-2*

Alle Links wurden zuletzt am 11.03.2019 geprüft.