21 CFR Part 11 Compliance - Checkliste

Das Industrie 4.0 – System

Gesetz (§)	Schlagwort	Umsetzung in DOQ	Status
11.10	Kontrollen für geschlossene Systeme	DOQ wurde als geschlossenes System entworfen, kann aber auch als offenes System genutzt werden.	✓
11.10a	Validierung von Systemen	LA2 hat DOQ gemäß IEC 62304 bzw. GAMP5 validiert und verifiziert. Mit frei definierbaren Wertgrenzen-Checks und einer durchgängigen Audittrail-Funktionalität werden gültige oder veränderte Daten erkannt und gesichert. Wir stellen unseren Kunden eine qualitätsgesicherte Dokumentation von Softwareupdates und Konfigurationsänderungen zur Verfügung, die Sie in ihrem Change Management Prozess (Softwarevalidierung, bzw. IQ/OQ/PQ) nutzen können.	✓
11.10b	FDA Kopien	Alle qualitätsrelevanten Informationen sind sowohl elektronisch als auch in menschenlesbarer Form vorhanden.	✓
11.10c	Schutz und Wiederherstellbarkeit	Zum Schutz der Aufzeichnungen und zur Gewährung des zeitnahen Zugriffs während der gesetzlichen Aufbewahrungsfristen steht eine flexibel integrierbare Archivierungsschnittstelle zur Verfügung. DOQ kann zusätzlich einfach in den Backup-Prozess beim Kunden integriert werden. Als Datenformat wurde das von der International Organization for Standardization (ISO) definierte Langzeitformat PDF/A (ISO 19005) gewählt. Die Sicherung der Daten kann somit ab der Dateneingabe bis zum Zeitpunkt der Archivierung sichergestellt werden. Gesetzliche Archivierungsfristen können so eingehalten werden.	✓
11.10d	Beschränkung des Systemzugriffs für berechtigte Personen	Der Zugang zur DOQ ist nur autorisierten Personen mit individuellem Login und Passwort gestattet. Passwortgültigkeit, automatische Passwortsperrung bei mehrfach falscher Eingabe und anschließender Freigabe durch einen Administrator sind nur einige der DOQ-Sicherungsfunktionalitäten.	✓
11.10e	Audittrails	Alle qualitätsrelevanten Daten besitzen einen Audittrail. Der Audittrail dokumentiert userspezifisch und sekundengenau alle Änderungen. Die unveränderbaren Audittrails stehen dabei sowohl elektronisch als auch in menschenlesbarer Form zur Verfügung. Sie besitzen die gleiche Aufbewahrungsdauer wie die zugrunde liegenden Daten. Der Audittrail in DOQ ist eine wesentliche Komponente, um die durchgängige Datenintegrität sicherzustellen.	✓
11.10f	Reihenfolge	Das System besitzt die Möglichkeit, feste (Prozess-)Abläufe zu definieren und stellt dabei zusätzlich über ein umfangreiches Monitoring sicher, dass diese auch eingehalten und kontrolliert werden können.	✓
11.10g	Zugangsprüfung	DOQ besitzt ein umfangreiches Rechte-/Rollenkonzept, welches allen 21 CFR Part 11 Anforderungen gerecht wird.	✓
11.10h	Device Checks	Das System verfügt über validierte und verifizierte Eingangs- und Ausgangsschnittstellen. Webservicebasiert werden die Daten eingelesen, bzw. im XLS-Format sicher zur Verfügung gestellt.	✓
11.10i	Ausbildung	Alle an der Erstellung von DOQ beteiligten Spezialisten sind sicher im Umgang mit den verschiedensten Regelwerken der Computersystemvalidierung (CSV) und darüber hinaus selbstverständlich auch in 21 CFR Part 11 geschult. Über rollenbasierte Schulungen und Bedienungsanleitungen wird sichergestellt, dass alle Personen die DOQ pflegen oder nutzen, die richtige Ausbildung, Schulung und Erfahrung besitzen, um die entsprechenden Aufgaben durchführen zu können.	✓
11.10j	Politik (Etablierung und Einhaltung schriftlich festgelegter Normen)	Neben den in 11.10i skizzierten Punkten, unterstützen wir Sie gerne bei der Umsetzung und Aktualisierung vorhandener Arbeits-/Verfahrensanweisungen und Policies.	✓
11.10k	Kontrolle der Dokumentation	Ein definiertes Kontrollverfahren der Validierungs-/Verifikationsdokumentation sowie die versionierte, audittrail-gesicherte und der Software zugeordnete (getestete) Bedienungsanleitung stellen diesen Punkt sicher.	✓
11.30	Kontrollen für offene Systeme	DOQ ist ein geschlossenes System, welches jedoch auch offen genutzt werden kann. Durch die Möglichkeit der Verschlüsselung zwischen dem Ort der Entstehung der Daten und Ort der Speicherung der Daten sowie der möglichen Einbindung von kryptographischen Methoden bei der Signaturerstellung kann dies einfach geschehen.	✓

21 CFR Part 11 Compliance - Checkliste

Das Industrie 4.0 – System

Gesetz (§)	Schlagwort	Umsetzung in DOQ	Status
11.50a/b	Information über die Unterschrift und Form der Unterschrift	Alle unterschriebenen elektronischen Aufzeichnungen werden mit der Electronic Signature verbunden und enthalten folgende Informationen: 1) Eindeutige Namensbezeichnung des Unterzeichners 2) Das Datum und die Uhrzeit zu der die Unterschrift geleistet wurde 3) Die mit der Unterschrift verbundene Bedeutung (wie z.B. Review, Genehmigung, Verantwortung oder Autorenschaft) Ein noch höherer Sicherheitslevel des Unterschriftenprozess wird u.a. durch die Möglichkeit - der Einsicht aller signaturrelevanten Vorgänge im System (vor der Signatur) - einer möglichen protokollierten Ablehnung inkl. Unterschriftsbestätigung - jederzeit zu signieren bzw. die Signaturvorgänge auch "bündeln" zu können - nach einem software-/hardwarebasierten Systemabsturz erneut lückenlos elektronisch signieren zu können, erreicht.	✔
11.70	Hybridsysteme	In DOQ werden derzeit keine Hybride verwendet.	✔
11.100a	Einzigartigkeit der Unterschrift	Jede elektronische Signatur ist eindeutig einem Benutzer zugeordnet. Sie ist einzigartig, d.h. sie kommt nur einmal im System vor und kann nicht durch andere Personen verwendet werden (auch nicht durch Administratoren!).	✔
11.100b und 11.100c	Identität der Person und Anzeige bei der FDA	Anwender sind verpflichtet bei der FDA anzuzeigen, dass ein System eingesetzt wird, mit dem nach CFR 21 Part 11 gearbeitet und signiert wird. Sofern angefordert, muss nachgewiesen werden, dass die Identität des jeweiligen Unterzeichners geprüft wurde und der Unterzeichner die Bedeutung der elektronischen Signatur kennt. Stellen Sie sicher, dass die Vorgaben der FDA gewährleistet sind. Bei dieser nichtfunktionalen Forderung unterstützen wir Sie gerne während des Prozesses der DOQ-Einführung.	✔
11.200a	Nicht biometrische elektronische Unterschriften	Die elektronische Unterschrift im System beruht nicht auf biometrischen Verfahren. Deswegen werden mit der Forderung nach ID und Passwort zwei verschiedene Komponenten zur Identifizierung verwendet. Ein Passwort-wechsel ist jederzeit möglich.	✔
11.200b	Biometrische Unter-schriften	s. 11.200a, daher trifft dieser Punkt nicht zu.	✔
11.300a	Beibehaltung der Einzigartigkeit einer Kombination aus Identifizierungscode und Passwort	Das Login ist eindeutig und kann im System nur einmalig vergeben werden.	✔
11.300b	Änderung und Alterung von Passwörtern	Es existieren vielfältige Möglichkeiten der Passwortalterung/-änderung sowie die Möglichkeit der Accountsperrung durch Administratoren.	✔
11.300c	Befolgung von Verlust-Management-Verfahren	Marken, Karten oder sonstige Identifizierungshardware werden derzeit nicht bei diesem System eingesetzt.	✔
11.300d	Erkennen der unbefugten Nutzung von Passwörtern	Anwender werden nach mehrmaliger Falscheingabe des Passwortes automatisch gesperrt. Die Freischaltung ist danach nur durch den Administrator möglich. Die Basis für die Erkennung von Anmeldemissbrauch ist somit gegeben und kann im Eintrittsfall ans Management weitergegeben werden.	✔
11.300e	Regelmäßiges Überprü-fen bei der Verwendung von Marken/ Karten/ sonstiger Hardware	Marken, Karten oder sonstige Identifizierungshardware werden derzeit nicht bei diesem System eingesetzt.	✔

✔ erfüllt ✔ nicht relevant ✖ nicht erfüllt

21 CFR PART 11 COMPLIANCE IST GEGEBEN