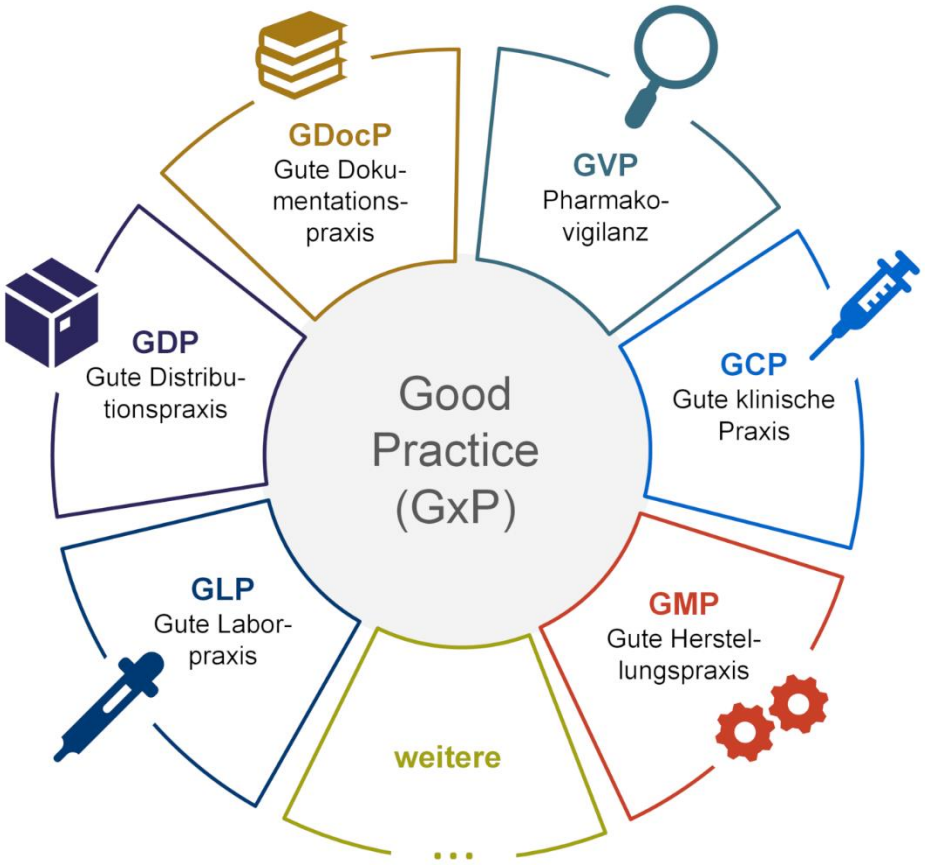
Inhalte:



GxP-Anforderungen

Tabelle 1: Auflistung der GxP-Anforderungen, kurze Inhaltsbeschreibung, Verweis auf Regularien und Realisierungen der Anforderungen in roXtra

Ref. Nr.	GxP-Anforderungen	Inhalte	Regularien	roXtra Realisierungen
A 1.	**Benutzerkennung, Zugangsdaten, Kennwörter**	• Einzigartigkeit jeder Kombination aus Benutzerkennung und Passwort → nur einmal vergeben • regelmäßig überprüft oder Passwörter zurückgenommen (um z. B. Veralten von Passwörtern zu verhindern)	21 CFR PART 11 – Teil C, Abs. 11.300	• Die Einzigartigkeit der Benutzerkennung ergibt sich in roXtra durch die Kombination aus Benutzername und Domain. Innerhalb einer Domain kann ein Benutzername nur ein Mal vergeben werden. Für **lokale Benutzer** existiert eine lokale Domain. Für **Benutzer, die den roXtra IDP-Connector** verwenden, gilt die jeweilige Windows/Azure Domain. • Kennwortrichtlinien Für **lokale Benutzer** können Kennwortrichtlinien durch Benutzer mit Rechten zur Benutzerverwaltung (Administration) festgelegt werden. Neben Bestandteilen des Kennworts und der Kennwortlänge, können auch Zeiträume für die Gültigkeit (und damit Erneuerungszyklen) festgelegt werden. Screenshot 1 zeigt die möglichen Systemeinstellungen für die Festlegung von Kennwortrichtlinien in roXtra. Weitere Informationen können dem roXtra Benutzer-Handbuch entnommen werden. Für **Benutzer, die den roXtra IDP-Connector** verwenden, erfolgt auch die Festlegung von Kennwortrichtlinien innerhalb der Windows Active Directory Oberfläche. Aus roXtra heraus können diese Einstellungen nicht geändert werden.

		• Verlustverfahren → Karten und anderen Vorrichtungen, die mit Benutzerkennungs- oder Passwortinformationen versehen sind, die Berechtigung entziehen.		• Änderung des Kennwortes Ist eine Änderung des Kennwortes notwendig (z. B. aufgrund von Veralterung oder Verlust), kann dies, bei **lokalen Benutzern,** durch den betroffenen Benutzer selbst oder einen Benutzer mit Rechten zur Benutzerverwaltung (Administration) in roXtra erfolgen. Der Administrator kann ein neues Kennwort festlegen und/oder die Erstellung eines neuen Kennwortes bei der Anmeldung in roXtra erforderlich machen. Bei **Benutzern, die den roXtra IDP-Connector** verwenden, entsprechen die roXtra-Logindaten den Windows/Azure-Anmeldedaten, somit erfolgt auch die Änderung von Kennwörtern innerhalb der Windows Active Directory Oberfläche. Aus roXtra heraus können diese Einstellungen nicht geändert werden.
		• Sicherheitsvorkehrungen → jeden Versuch der unbefugten Benutzung entdecken und diesen an die Sicherheitseinheit des Systems und im Bedarfsfall an die Unternehmensführung weiterleiten		• Sicherheitsvorkehrungen Um einem Brute-Force-Angriff entgegenzuwirken, wird, nachdem 10-mal fehlerhafte Zugangsdaten bei der Anmeldung in roXtra eingegeben wurden, der Zugang beim nächsten Versuch für 10 Minuten gesperrt. Zudem wird bei Verdacht auf einen Brute-Force-Angriff der Systemverantwortliche per Email benachrichtigt. Bei Verwendung des **roXtra IDP-Connectors** können zusätzliche Sicherheitsrichtlinien im Active Directory hinterlegt sein.
A 2.	**Befugte Personen,**	• nur geeignete und befugte Personen dürfen genehmigen	EU-GMP Leitfaden (EudraLex) Teil I; Kapitel 4 4.3, 4.9	• Rechte und Rollen können durch Benutzer mit Rechten zur Benutzerverwaltung (Administration) verwaltet werden. Weitere Informationen können dem roXtra Benutzer-Handbuch, sowie dem Administrator-Handbuch entnommen werden.

	Zugangsbe-schränkung, Sicherheit	• Zugang zum System sollte durch Kennwörter oder auf andere Weise geschützt sein • Umfang der Sicherheitsmaß-nahmen abhängig von Kritikalität des computergestützten Systems	Anhang 11 zum EU-GMP Leitfaden (EudraLex) 12. Sicherheit 12.1, 12.2, 12.3, 12.4 21 CFR PART 11 – Teil B, Abs. 11.10 Teil C, Abs 11.300	• Der Zugang zum System erfolgt personengebunden mittels roXtra Bearbeiter-Lizenz oder roXtra Leser-Lizenz. Der Zugang ist hierbei durch die Eingabe von Benutzername und Kennwort geschützt. Zudem besteht die Möglichkeit Dokumente zum Lesen für sogenannte „roXtra Public-Leser“ freizuschalten. Diese Funktion ermöglicht den Gastzugang für den gleichzeitigen anonymen Zugriff von beliebig vielen Mitarbeitern, sollte jedoch im Rahmen einer Risikoanalyse beurteilt und ggfs. im GxP-Umfeld vermieden werden. Für Supporttätigkeiten steht über den Benutzer „System“ ein Zugang zum jeweiligen roXtra System beim Kunden zur Verfügung. Der Support erfolgt durch befugte und geschulte Mitarbeiter und ist durch die Verwendung von kundenspezifischen Tageskennwörtern geschützt. • Aufz… …ngen bzw. der Benutzerstruk-Ä… …dit Trail dokumentiert (siehe … **…n werden.**).