

Inhalt

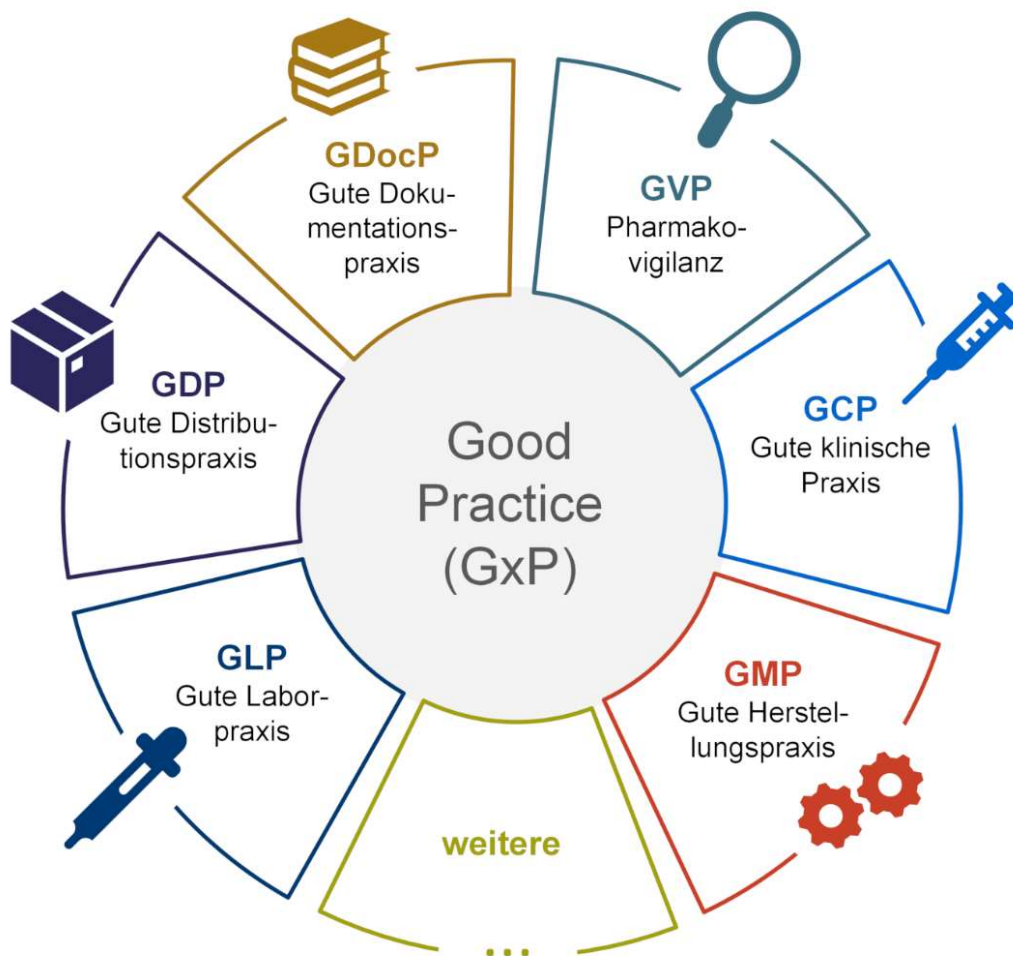
1	Überblick.....	2
2	GxP-Anforderungen.....	3
3	Anlagen.....	15
3.1	Begriffsklärung.....	15
3.2	Screenshots.....	16
3.3	Regularien.....	18

1 Überblick

Der Abschnitt **2 GxP-Anforderungen** beinhaltet eine Auflistung der gängigen GxP-Anforderungen sowie jeweils eine kurze Inhaltsbeschreibung und den Verweis auf die Regularien.

Das Kapitel **3 Anlagen** beinhaltet:

- **Begriffsklärung:** kurze Erläuterung wichtiger Begriffe, die in Tabelle 1 in der Spalte „roXtra Realisierungen“ verwendet werden
- **Screenshots:** Beispiele und Veranschaulichungen der roXtra Benutzeroberfläche
- **Regularien:** vollständige Abschnitte aus Regularien, auf die in Tabelle 1 verwiesen wurde



2 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	<ul style="list-style-type: none"> ▪ Einzigartigkeit jeder Kombination aus Benutzerkennung und Passwort → nur einmal vergeben ▪ regelmäßig überprüft oder Passwörter zurückgenommen (um z. B. Veralten von Passwörtern zu verhindern) ▪ Verlustverfahren → Karten und anderen Vorrichtungen, die mit Benutzerkennungs- oder Passwortinformationen versehen sind, die Berechtigung entziehen. 	21 CFR PART 11 – Teil C, Abs. 11.300	<ul style="list-style-type: none"> ▪ Die <u>Einzigartigkeit der Benutzerkennung</u> 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. ▪ <u>Kennwortrichtlinien</u> 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. ▪ <u>Änderung des Kennwortes</u> 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

Ref. Nr.	GxP-Anforderungen	Inhalte	Regularien	roXtra Realisierungen
		<ul style="list-style-type: none"> ▪ Sicherheitsvorkehrungen → jeden Versuch der unbefugten Benutzung entdecken und diesen an die Sicherheitseinheit des Systems und im Bedarfsfall an die Unternehmensführung weiterleiten 		<p>und/oder die Erstellung eines neuen Kennwortes bei der Anmeldung in roXtra erforderlich machen.</p> <p>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.</p> <ul style="list-style-type: none"> ▪ <u>Sicherheitsvorkehrungen</u> 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, Zugangsbeschränkung, Sicherheit	<ul style="list-style-type: none"> ▪ nur geeignete und befugte Personen dürfen genehmigen ▪ Zugang zum System sollte durch Kennwörter oder auf andere Weise geschützt sein ▪ Umfang der Sicherheitsmaßnahmen abhängig von Kritikalität des computergestützten Systems 	<p>EU-GMP Leitfaden (EudraLex) Teil I; Kapitel 4 4.3, 4.9</p> <p>Anhang 11 zum EU-GMP Leitfaden (EudraLex) 12. Sicherheit 12.1, 12.2, 12.3, 12.4</p> <p>21 CFR PART 11 – Teil B, Abs. 11.10 Teil C, Abs 11.300</p>	<ul style="list-style-type: none"> ▪ <u>Rechte und Rollen</u> können durch Benutzer mit Rechten zur Benutzerverwaltung (Administration) verwaltet werden. Weitere Informationen können dem roXtra Benutzer-Handbuch, sowie dem Administrator-Handbuch entnommen werden. ▪ Der <u>Zugang zum System</u> 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.

Ref. Nr.	GxP-Anforderungen	Inhalte	Regularien	roXtra Realisierungen
		<ul style="list-style-type: none"> ▪ Aufzeichnung von Erteilung, Änderung und Entzug von Zugriffsberechtigungen ▪ Identität des Anwenders, der Daten eingibt, ändert, bestätigt oder löscht, sollte mit Datum und Uhrzeit aufgezeichnet werden 		<p>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.</p> <ul style="list-style-type: none"> ▪ Werden <u>Änderungen an Zugriffsberechtigungen</u> bzw. der Benutzerstruktur durchgeführt, wird dies im zugehörigen Audit Trail dokumentiert (siehe Screenshot 2). ▪ Die Identität des Anwenders, der Daten eingibt, ändert, bestätigt oder löscht, wird mit Datum und Uhrzeit aufgezeichnet (siehe Screenshot 2). Bei Benutzern, die den roXtra IDP-Connector verwenden, können diese Änderungen in roXtra nicht protokolliert werden, da Stammdaten hierbei ggf. unter der Kontrolle des jeweiligen Systems liegen.

Realisierung von GxP-Anforderungen in roXtra

Das vollständige Dokument ist Bestandteil der Musterdokumentation zur Validierung von roXtra. Gerne erstellen wir Ihnen hierzu ein unverbindliches Angebot. Kontaktieren Sie uns einfach per E-Mail an service@roxtra.com oder telefonisch unter +49 (7161) 505 700.

