

pharmind



news

Nachrichten  
und Mitteilungen  
Official  
Communications

Sonderausgabe  
Elektronische Signaturen

eine Kooperation  
zwischen APV und ECV

# Elektronische Signaturen

**Empfehlung der Fachgruppe Informationstechnologie  
der Arbeitsgemeinschaft für Pharmazeutische Verfahrenstechnik e.V. (APV)  
sowie der Expertengruppe Elektronische Signatur**

---

**Autoren: APV-Fachgruppe Informationstechnologie und Expertengruppe Elektronische Signatur**

Jannis Batoulis, Bayer Business Services GmbH, Leverkusen  
Konstantin Clevermann, IDS Scheer AG, Düsseldorf  
Christoph Hornberger, EMR Engineering GmbH, Ingelheim  
Ralf Hössel, Boehringer Ingelheim Pharma GmbH & Co KG, Ingelheim  
Robert Jaster, Boehringer Ingelheim Pharma GmbH & Co KG, Biberach  
Eberhard Klappauf, COMLINE Computer + Softwarelösungen AG, Hamburg  
Wolfgang Kleemann, Roche Diagnostics GmbH, Penzberg  
Thomas Linz, Bayer Schering Pharma AG, Berlin  
Jörg Schwamberger, Merck KGaA, Darmstadt  
Martin Schulz, F. Hoffmann-La Roche Ltd, Basel  
Dieter Weiser, Nycomed GmbH, Konstanz

## Danksagung

**Wir bedanken uns für die Unterstützung und Beratung zu einzelnen Themen, die uns bei der Ausarbeitung dieser Empfehlung äußerst hilfreich waren bei:**

Stefan Engel-Flechsig, Rechtsanwalt, Bonn  
Lothar Helling, Boehringer Ingelheim Pharma GmbH & Co KG, Ingelheim  
Marko Lange, SAP AG, Walldorf  
Christoph Roller, SAP AG, Walldorf

## Inhaltsverzeichnis

1	Einleitung	5
2	Grundsätzliche Überlegungen	5
2.1	Bedeutung der Unterschrift im Prozess und Anwendungsbeispiele	5
2.2	Regulatorische Anforderungen GMP, GLP, GCP	6
2.2.1	GMP-Bereich	6
2.2.2	Medical Devices	8
2.2.3	GLP-Bereich	10
2.2.4	GCP-Bereich	11
2.2.5	Arzneimittelzulassung	11
2.3	Juristische Betrachtung	12
2.3.1	Deutsches Signaturgesetz (SigG)	12
2.3.2	21 CFR Part 11	14
2.4	AMWHV und AMG: Auswirkung der juristischen Betrachtungen auf regulatorische Anforderungen in den Bereichen GMP, GLP, GCP	15
2.5	Risikobasierter Ansatz	16
2.6	Schlussfolgerung	20
3	Organisation	21
3.1	Rechtsverbindlichkeit	21
3.1.1	Rechtsverbindlichkeit im Verhältnis Mitarbeiter – Firma	21
3.1.2	Rechtsverbindlichkeit im Verhältnis Firma – Behörde (hier: FDA)	22
3.2	Manipulationsschutz	22
3.3	Regelungen zum Betrieb	22
4	Anforderungen an die Validierung	23
4.1	User Requirements, Spezifikation, Design, Risikoanalyse	23
4.1.1	Allgemeines	23
4.1.2	Änderungen signierter Daten	24
4.2	Entwickler- und Abnahmetests	24
4.3	Systembetrieb	25
4.3.1	Beschreibung fachlicher Abläufe	25
4.3.2	Schulung	25
4.3.3	Berechtigungskonzept	25
4.3.3.1	Authentisierung/Authentifizierung	25
4.3.3.2	Autorisierung/Verwaltung der Berechtigungen	26
4.3.4	Änderungskontrolle (Change Control)	27
4.3.5	Störungen	27
4.3.6	Abweichungen	27
4.3.7	Datensicherung und Wiederherstellung	27
4.3.8	Regelmäßige Systemüberwachung (Monitoring)	27
4.3.9	Archivierung	27
4.3.10	Sicherheit und Notfallkonzept	28
4.3.11	Periodische Überprüfungen	28
4.4	Außerbetriebnahme	28
5	Erläuterungen zur Public-Key-Infrastruktur (PKI)	28
6	Glossar	29
7	Abkürzungen	30
8	Literaturhinweise	31
9	Nützliche Links und Adressen	31
10	Anhang	31

## Zusammenfassung

Der Nutzen der Anwendung elektronischer Signaturen wird zunehmend deutlicher. Sie sichert einen durchgängigen elektronischen Workflow und erhöht damit auch die Produktsicherheit. Die gesetzlichen Rahmenbedingungen im regulierten Umfeld ermöglichen durchaus ihren Einsatz. Allerdings besteht Unsicherheit bei der Wahl der geeigneten Form der elektronischen Signatur. Klarheit lässt sich hier erreichen, wenn zusätzlich zu den gesetzlichen Anforderungen auch die unterstützten Abläufe sowie die mit dem jeweiligen System verbundenen Risiken betrachtet werden. Dabei zeigt sich: Nur in wenigen Fällen ist die qualifizierte elektronische Signatur erforderlich, um ein angemessenes Maß an Sicherheit und Vertrauenswürdigkeit zu gewährleisten.

## 1 Einleitung

Im regulierten pharmazeutischen Umfeld müssen in normalen Geschäftsprozessen Unterschriften mit unterschiedlichster Bedeutung und Tragweite geleistet werden. Beispielsweise zählen hierzu die Erstellung und Freigabe von Arbeits- bzw. Verfahrensanweisungen, die Freigabe von Prüfvorschriften, die Freigabe von Herstellungsberichten nach der Produktion oder die Prüffreigabe von Rohstoffen, Bulkware oder Endprodukten im Labor. Diese Unterschriften – auch mit ihrer unterschiedlichen Tragweite – werden an verschiedenen Stellen im Deutschen Arzneimittelgesetz (AMG), in der Arzneimittel- und Wirkstoffherstellungsverordnung (AMWHV) oder in den EU-Regularien (z. B. Good Manufacturing Practice for Medicinal Products oder in Good Laboratory Practice Regularien) gefordert.

In diesen deutschen bzw. europäischen Richtlinien sind jedoch nur sehr wenige Vorgaben zu finden, wie die Unterschriften ggf. auch in elektronischer Form geleistet werden können.

Für den US-amerikanischen Bereich hingegen ist der 21 CFR Part 11 der Food and Drug Administration (FDA) mit seinen Anforderungen zur elektronischen Signatur (Electronic Signatures) seit 1997 in Kraft.

Obwohl viele der im regulierten Umfeld eingesetzten IT-Systeme elektronische Signaturen unterstützen und keine Regelung existiert, die den Einsatz elektronischer Signaturen in irgendeinem Geschäftsfeld untersagt, wird dies nach wie vor in der pharmazeutischen Industrie noch wenig genutzt. Dabei gibt es kaum Gründe, auf die Vorteile der elektronischen Datenhaltung inkl. des elektronischen Handlings der Workflows und der Freigabeprozesse zu verzichten. Schließlich erhöht dies die Verfügbarkeit, die Recherchierbarkeit der Daten und reduziert die Fehleranfälligkeit.

Zur Einführung und Nutzung von elektronischen Signaturen im regulierten Umfeld herrscht nach wie vor große Unsicherheit bzgl. der Fragen,

- welche juristischen Grundlagen insbesondere in Deutschland zu berücksichtigen sind,
- welche technischen Maßnahmen zu treffen sind,
- inwieweit die technischen Lösungen behördlich akzeptiert werden,
- welche organisatorischen Verfahren innerbetrieblich zu regeln sind.

Viele missverstehen den Einsatz von elektronischen Signaturen als eine ausschließlich technische Lösung. Sie wird als eine zusätzliche Passwort-Abfrage oder als ein Identifikationsverfahren (Authentifizierung) in einem IT-System betrachtet. Übersehen wird dabei, dass stets der gesamte Prozess und der organisatorische Rahmen betrachtet werden müssen, damit die elektronische Signatur der handschriftlichen gleichgesetzt werden kann.

Vor diesem Hintergrund bietet die APV-Fachgruppe "Informationstechnologie" mit dieser Empfehlung sowohl der pharmazeutischen Industrie als auch den Aufsichtsbehörden Unterstützung an. Mitte 2006 hat die Fachgruppe bereits eine erste Stellungnahme dazu publiziert (Pharm. Ind. 68, Nr. 5, S. 552 ff.; 2006). Nachfolgend wird die vollständige Empfehlung veröffentlicht.

Eine wesentliche Fragestellung ist dabei die Berücksichtigung der deutschen Signaturgesetzgebung sowie der Abgleich mit den entsprechenden Anforderungen der EU und der FDA. Mit noch höherer Priorität wird das eigentliche Arbeitsumfeld betrachtet: Wie sind die Risiken solcher Lösungen im Hinblick auf die pharmazeutische Qualität zu bewerten? Welche Schlüsse sind daraus für die verschiedenen Lösungsmöglichkeiten zu ziehen?

## 2 Grundsätzliche Überlegungen

### 2.1 Bedeutung der Unterschrift im Prozess und Anwendungsbeispiele

Die Unterschrift kennzeichnet die dokumentierte Übernahme der Verantwortung. Sie wird benötigt, wenn ein Ergebnis abgeschlossen und bestätigt wird oder wenn die Einwilligung zu weiteren Arbeiten erfolgen soll.

Im folgenden werden einige Beispiele aus unterschiedlichen Bereichen vorgestellt:

#### Forschung

- Labor-Journaleinträge werden unterschrieben. Die schriftliche Dokumentation der Planung, Durchführung und Auswertung von Experimenten, aber auch die Formulierung von Ideen für künftige Vorhaben ist für die Zuerkennung eines möglichen Patentbesitzes wichtig.

### Entwicklung

- Prüfpläne beschreiben die Ziele und die experimentelle Gesamtplanung der Durchführung einer Labor-Prüfung und werden vom Prüfleiter unterschrieben.
- Die Durchführung einer klinischen Prüfung erfordert die vorherige Genehmigung der zuständigen Ethik-Kommission. Dazu muss ihr eine vorgegebene Liste von unterzeichneten Dokumenten vorgelegt werden. Weitere Dokumente werden im Rahmen einer klinischen Prüfung unterschrieben wie z. B. Clinical Development Plan, Data Management Plan, Investigator's Brochure, Clinical Study Protocol, Statistical Analysis Plan, Monitoring Manual.
- Zur Zulassung von Arzneimitteln wird ein Gutachten eingefordert, in dem die Kontrollmethoden, Prüfungsergebnisse und Rückstandsnachweisverfahren zusammengefasst und bewertet werden. Dieses Gutachten wird von Sachverständigen unterschrieben.

### Produktion

- Die Herstellungsvorschriften werden mit Unterschrift freigegeben.
- Das Protokoll der Herstellung von Chargen eines Arzneimittels ist zu unterschreiben.
- Die Freigabe der Endprodukte ist zu unterschreiben.

### Qualitätskontrolle/-sicherung

- Prüfvorschriften und Arbeitsanweisungen (SOPs) werden durch eine Unterschrift gültig.
- Die Verwendungsfreigabe von Ausgangsstoffen für die Produktion ist zu unterzeichnen.
- Die in QM-Systemen geforderten Schulungsnachweise sollen in unterschriebener Form vorgelegt werden können.
- Ein Audit-Bericht wird unterschrieben.

### Erstellung und Betrieb von DV-Systemen, Laborgeräten oder Anlagen

- Wichtige Dokumente bei der Erstellung eines DV-Systems werden durch Unterschrift abgenommen. Dazu gehören im allgemeinen der Validierungsplan, die Qualifizierungsdokumente, Spezifikationen und Testdokumentation.
- Beim Betrieb eines DV-Systems werden Änderungen und Erweiterungen nach einem vorher festgelegten Change Control-Verfahren durchgeführt. Die Sicherstellung der Qualität bedingt im allgemeinen einen formalisierten Prozess, der durch unterschriebene Dokumente gelenkt wird.
- Zugehörige SOPs und Dokumente zum Life Cycle des Systems oder von Anlagen (z. B. Pläne für den Betrieb, die Datensicherung, Zugangsberechtigungen und weitere) werden gemäß unternehmensinterner Regelungen unterschrieben.

Allen Beispielen ist eines gemeinsam:

Die Unterschrift bestätigt, dass ein geforderter Arbeitsprozess ordnungsgemäß abgeschlossen wurde. Diese Unterschrift wird nicht immer gesetzlich verlangt. So gibt es z. B. keine expliziten gesetzlichen Vorgaben darüber, welche Dokumente bei der Entwicklung eines DV-Systems zu unterschreiben sind. Letztlich sind die firmeneigenen Arbeitsanweisungen maßgeblich, und diese müssen sicherstellen, dass die gesetzlichen Bestimmungen erfüllt werden. Sie können aber aus Gründen der Qualität oder Zweckmäßigkeit auch darüber hinausgehen.

## 2.2 Regulatorische Anforderungen GMP, GLP, GCP

Im Rahmen der nachstehenden Ausführungen werden zunächst einige zugrundeliegende Regularien genauer betrachtet, um die jeweilige Anforderung an eine Unterschrift transparent zu machen. Es wird darauf hingewiesen, dass an einigen Stellen eine „Unterschrift mit Datum“ gefordert wird, an anderen Stellen hingegen ein „Kürzel“ oder „Initial“ genügt. Dabei kann weder ein Anspruch auf Vollständigkeit der ausgewählten Regularien noch auf eine absolut vollständige Überprüfung der einzelnen Regularien erhoben werden. Im Zweifelsfall müssen die entsprechenden Dokumente sowohl textlich als auch der Vollständigkeit halber nachgeschlagen werden. Weitere Regularien, die teilweise im folgenden nur namentlich erwähnt werden, sind z. B. auch im GAMP-Good Practice Guide „Risk Based Approach to Electronic Records & Signature“ zu finden. Dort wurden einige Regularien zusätzlich analysiert. Eine grundsätzlich andere Auslegung als die hier beschriebene ist jedoch auch in anderen Regelwerken nicht zu erwarten. Aus diesem Grund wurde auf eine weitergehende Analyse verzichtet.

### 2.2.1 GMP-Bereich

Im GMP-Bereich sind im wesentlichen das Arzneimittelgesetz (AMG), die Arzneimittel- und Wirkstoffherstellungsverordnung (AMWHV), der EG-GMP-Leitfaden sowie für den US-Export die Paragraphen des 21 CFR Part 210/211 als regulatorische Vorgaben relevant.

Auf die Verordnungen zum AMG wird nicht näher eingegangen, da dies den Rahmen dieser Empfehlung sprengen würde.

Im AMG selbst ist nur bei der Zulassung von Arzneimitteln – in § 24 Sachverständigengutachten – von einer Unterschriftspflicht die Rede; siehe hierzu Kapitel 2.2.4 (GCP)

Die Anforderungen des EU-GMP-Leitfadens sind durch die Formulierungen im AMWHV abgedeckt und müssen gleichfalls nicht weiter beschrieben werden.

In der AMWHV, die Ende 2006 die Betriebsverordnung für pharmazeutische Unternehmer (PharmBetrV) abgelöst hat, wird an wenigen Stellen eine „Unterschrift“ oder ein „Unterzeichnen“ gefordert. Eine Übersicht zeigt Tab. 1 (eine ausführliche Auflistung der entsprechenden Textpassagen findet sich im Anhang, Tabelle 1).

Tab. 1: Erwähnung von Unterschriften/Unterzeichnungen in der AMWHV.

§§	Absatz / Thema	Gefordert
<b>Abschnitt 3: Arzneimittel, Blutprodukte, Produkte menschlicher Herkunft</b>		
13 Herstellung	Herstellprotokoll	Datum und Unterschrift
14 Prüfung	Prüfprotokoll	Datum und Unterschrift
17 Inverkehrbringen (2)	Kontrollbericht (gemäß Vorschrift eines Mitgliedstaates der EU bzw. Vertragsstaates)	Unterzeichnung
<b>Abschnitt 4: Wirkstoffe nicht-menschlicher Herkunft</b>		
22 Herstellung	Herstellprotokoll	Datum und Unterschrift
23 Prüfung	Prüfprotokoll	Datum und Unterschrift
25 Inverkehrbringen (4)	Bei Zwischenprodukten und Wirkstoffen: Prüfprotokoll zur Identitätsprüfung	Ordnungsgemäße Unterzeichnung

An verschiedenen Stellen werden sogenannte „vorher erstellte schriftliche Anweisungen“ gefordert. Gemeint sind Prüfanweisungen, Herstellenanweisungen und Anweisungen für das Inverkehrbringen. Interessant ist hier, dass in der neuen AMWHV (im Gegensatz zu den GLP-Anforderungen; s. u.) nicht explizit erwähnt ist, ob diese Anweisungen zu unterschreiben sind, sondern nur, wer für die Freigabe verantwortlich ist. Eine Übersicht (nicht vollständig) gibt Tab. 2 (eine ausführliche Auflistung der entsprechenden Textpassagen findet sich im Anhang, Tabelle 2).

Tab. 2: Erwähnung von schriftlichen Anweisungen in der AMWHV.

§§	Absatz / Thema	Gefordert
6 Hygienemaßnahmen	Hygieneplan und Hygieneprogramme	„schriftlicher Plan“
7 Lagerung und Transport	Verfahren zur Lagerung und Transport	„schriftlich festzulegen“
11 Selbstinspektion und Lieferantenqualifizierung	Verfahren zur Lieferantenqualifizierung	„schriftlich festzulegen“
12 Personal in leitender Stellung	Verantwortungsbereiche und Aufgaben	„schriftlich festzulegen“
13 und 22 Herstellung	Herstellungsanweisung	„schriftliche Anweisung“
14 und 23 Prüfung	Prüfanweisung	„schriftliche Anweisung“
16 und 25 Freigabe zum Inverkehrbringen	Anweisung zur Freigabe zum Inverkehrbringen	„schriftliche Anweisung“
19 und 28 Beanstandungen und Rückruf	Verfahren zum Rückruf	„schriftliche Anweisung“
24 Kennzeichnung	Verfahren zur Kennzeichnung von Zwischenprodukten oder Wirkstoffen	„schriftliche Anweisung“

Von Bedeutung für die weiteren Entscheidungen ist §10, Abs. 2, der AMWHV, da in diesem das Vorgehen ohne expliziten Verweis auf das Signaturgesetz vorgegeben wird.

10 (2) ... Wird ein System zur automatischen Datenverarbeitung oder -übertragung eingesetzt, so genügt statt der eigenhändigen Unterschrift der jeweils verantwortlichen Personen deren Namenswiedergabe, wenn in geeigneter Weise sichergestellt ist, dass nur befugte Personen die Bestätigung über die ordnungsgemäße Ausführung der jeweiligen Tätigkeiten vornehmen können.

Das bedeutet, dass für alle in der AMWHV geforderten Unterschriften die Wahlfreiheit bei der Auswahl einer geeigneten elektronischen Signatur gegeben ist. Die Bedeutung dieses Absatzes für die weiteren Ausführungen wird im Kapitel 2.3, „Juristische Betrachtung“, erläutert.

#### 21 CFR Part 210/211

Bei den cGMP-Regeln der FDA (21 CFR Part 210/211) ist im Zusammenhang mit den Ausführungen im Kapitel 2.3 zu beachten, dass diese Regelungen im EU-Raum nicht als „formal gültiges Gesetz“ anzusehen sind.

Im CFR Part 210/211 werden häufig die Begriffe „Approval“ und „Initial or Signature“ verwendet. An nur zwei Stellen (211.186 und 211.188) ist explizit eine „Signature“ verlangt.

Eine Übersicht wird in Tab. 3 gegeben (eine ausführliche Auflistung der entsprechenden Textpassagen findet sich im Anhang, Tabelle 3).

Tab. 3: 21 CFR Part 210/211 der FDA.

§§3	Absatz / Thema	Gefordert
211.22	Responsibilities of quality control unit	Approval
211.84	Testing and approval or rejection of components, drug product containers, and closures	Approval
211.100 (a)	Written procedures; deviations	Approval
211.160	General requirements for laboratory controls	Approval
211.182	Equipment cleaning and use log	Initial or signature
211.186 (a), (b) 8)	Master production and control records	Signed (full signature, handwritten)
211.188 (a)	Batch production and control records	Dated and signed
211.192	Production record review	Approval
211.194 (a), 7), 8)	Laboratory records	Initial or Signature

In analoger Weise könnte der 21 CFR Part 58 Good Laboratory Practice Regulations für den weiter unten stehenden GLP-Bereich ausgelegt werden (siehe Kapitel 2.2.3). Es wird empfohlen, bei Bedarf entsprechend vorzugehen.

#### Art der Unterschrift

In den o. g. Regularien werden unterschiedliche Formen der Unterschrift benannt. Wenn in deutschsprachigen Vorschriften von „ordnungsgemäßer Unterschrift“ oder „Datum und Unterschrift“ die Rede ist, ist sicherlich eine vollständige Unterschrift mit Datum gemeint. Dasselbe gilt für die Formulierungen „full signature handwritten“ oder „dated and signed“ und „approval“.

Zu den Anforderungen „Initial or signature“ ist im GAMP-„Good Practice Guide: A Risk-Based Approach to Compliant Electronic Records and Signatures“ die Interpretation zu finden, dass auch hier eine vollständige Unterschrift gemeint sei und dass das „or“ sich auf eine textliche Alternative des Begriffes bezieht. Nach Einschätzung der Autoren dieser APV-Empfehlung ist – insbesondere im Sinne eines „risk-based approach“ – gemeint, dass wahlweise entweder eine „signature“ (also eine vollständige Unterschrift) oder ein „initial“ (also nur ein Kürzel) benutzt werden kann. Weiteres hierzu siehe auch im Kapitel 2.5, „Risikobasierter Ansatz“, Absatz „Initial or Signature“.

**Fazit: Im Sinne des „risk-based approach“ sollte eindeutig geprüft und festgelegt werden, ob es sich bei dem elektronischen Bestätigungsvorgang um eine „Unterschrift“ oder nur um eine „Bestätigung mit Kürzel“ handelt.**

#### 2.2.2 Medical Devices

Im Bereich Medical Devices sind im Wesentlichen zu betrachten:

- Gesetz über Medizinprodukte (MPG)
- Directive 98/79/EC on in vitro diagnostic medical devices (Richtlinie 98/79/EG über In-vitro-Diagnostika)
- 21 CFR Part 820 Medical Devices cGMP

Bei Durchsicht dieser Regularien wurden keine wesentlich anderen Anforderungen gefunden, so dass diese auch nicht weiter analysiert wurden. Im MPG ist zwar an verschiedenen Stellen von einer Forderung nach „schriftlichem Nachweis“ die Rede, es wird jedoch nicht explizit nach einer Unterschrift verlangt. Nachfolgend wird bezüglich elektronischer Signaturen analog geschlossen (ausgewählte Beispiele hierzu siehe in Tab. 4).

Tab. 4: Auszüge aus dem MPG.

§§	Absatz / Thema	Gefordert
16 Erlöschen, Rücknahme, Widerruf und Ruhen der Akkreditierung und Benennung	(1) Akkreditierung und Benennung erlöschen mit der Einstellung des Betriebes der benannten Stelle oder durch Verzicht. Die Einstellung oder der Verzicht sind der zuständigen Behörde unverzüglich schriftlich mitzuteilen	Schriftliche Mitteilung
19 Klinische Bewertung, Leistungsbewertung	(1) 1. Daten aus der wissenschaftlichen Literatur, die die vorgesehene Anwendung des Medizinproduktes und die dabei zum Einsatz kommenden Techniken behandeln, sowie einen schriftlichen Bericht, der eine kritische Würdigung dieser Daten enthält, oder ...	Schriftlicher Bericht
20 Allgemeine Voraussetzungen zur klinischen Prüfung	(2) Eine Einwilligung nach Absatz 1 Nr. 2 ist nur wirksam, wenn die Person ... die Einwilligung selbst und schriftlich erteilt hat	Schriftliche Einwilligung
31 Der Medizinprodukteberater	(4) Der Medizinprodukteberater hat Mitteilungen ... oder sonstige Risiken bei Medizinprodukten schriftlich aufzuzeichnen und unverzüglich ... schriftlich zu übermitteln	Schriftlich zu übermitteln

Interessanterweise verlangt die IVD-Direktive nicht direkt eine Unterschrift, sie fordert aber an verschiedenen Stellen

- approved design,
- approved quality system,
- approved device.

Im 21 CFR Part 820.40 kann das „approved“ ein „date and signature“ bedeuten. Dies ist jedoch in der IVD-Direktive nicht explizit erwähnt, woraus sich dafür auch keine Forderung nach einer Unterschrift ableiten lässt.

Im 21 CFR Part 820 wird an verschiedenen Stellen „date and signature“ verlangt. Wichtig ist darin Absatz „820.40 Document Control“, in dem generell „approval including date and signature“ definiert wird. An verschiedenen anderen Stellen wird nur „approval“ oder „approved in accordance with 820.40“ gefordert. Einige ausgewählte Auszüge werden in Tab. 5 wiedergegeben.

Tab. 5: Auszüge aus 21 CFR Part 820.

§§	Absatz / Thema	Gefordert
820.30 Design Control	(c) Design Input and also (d) Design Output ... The approval, including the date and signature of the individual(s) approving the requirements, shall be documented.	Date and Signature
820.40 Document Control	(a) Document approval and distribution ... The approval, including the date and signature of the individual(s) approving the document, shall be documented. (b) Document Changes Change records shall include a description of the change, identification of the affected documents, the signature of the approving individual(s), the approval date, and when the change becomes effective.	Date and Signature
820.75 Process Validation	(a) The validation activities and results, including the date and signature of the individual(s) approving the validation and where appropriate the major equipment validated, shall be documented.	Date and Signature
820.80 Receiving, In-process and Finish Device Acceptance	(d) Final acceptance activities (2) the associated data and documentation is reviewed (3) the release is authorized by the signature of a designated individual(s); and (4) the authorization is dated.	Date and Signature

§§	Absatz / Thema	Gefordert
820.90 Nonconforming Product	(b) Nonconformity Review Documentation shall include the justification for use of nonconforming product and the signature of the individual(s) authorizing the use.	Signature
820.120 Device Labeling	(b) Labeling inspection. Labeling shall not be released for storage or use until a designated individual(s) has examined the labeling for accuracy including, where applicable, the correct expiration date, control number, storage instructions, handling instructions, and any additional processing instructions. The release, including the date and signature of the individual(s) performing the examination, shall be documented in the DHR.	Date and Signature

**Fazit: Im deutschen und europäischen Bereich wird zumindest an den oben analysierten Stellen nicht explizit eine Unterschrift verlangt. Diese Forderung stellt hingegen der Part 820.40 indirekt.**

### 2.2.3 GLP-Bereich

Im GLP-Bereich sind mehrere regulatorische Vorgaben zu beachten:

- Chemikaliengesetz
- EG-Richtlinie für die Anwendung der Grundsätze der Guten Laborpraxis
- OECD-GLP-Konsensdokumente
- Allgemeine Verwaltungsvorschrift zum Verfahren der behördlichen Überwachung der Einhaltung der Grundsätze der Guten Laborpraxis (ChemVwV-GLP)
- 21 CFR Part 58 Good Laboratory Practice Regulations (nicht weiter analysiert)

Die aufgeführten Regularien enthalten mit Blick auf Unterschriften etwa die gleichen Aussagen. Sie sind in Tab. 6 zusammengefasst (Details sind den Tabellen im Anhang zu entnehmen). An einigen Stellen wird explizit eine „datierte Unterschrift“ verlangt, an anderen Stellen dagegen lediglich ein Abzeichnen.

Tab. 6: Hinweise auf Unterschriften/Unterzeichnungen im GLP-Bereich (Zusammenfassung aus den Tabellen 4 bis 7 im Anhang).

	Absatz / Thema	Gefordert
Aufgaben des Prüfleiters	Prüfplan, Änderungen zum Prüfplan und Abschlussbericht zur Prüfung	Datierte Unterschrift
Aufgaben des QS-Personals	Erklärung zum Abschlussbericht des Prüfplanes	Unterzeichnung
Durchführung der Prüfung	Während der Prüfung erhobene Daten	Abzeichnen
Durchführung der Prüfung	Änderungen an Rohdaten	Kürzel
Bericht über die Prüfergebnisse	<ul style="list-style-type: none"> <li>• Bericht des örtlichen Versuchsleiters oder beteiligten Spezialisten,</li> <li>• Bericht eines Principal Investigators oder Wissenschaftlers</li> <li>• Abschlussbericht des Prüfleiters</li> <li>• Korrekturen und Änderungen des Abschlussberichtes</li> </ul>	Datierte Unterschrift

Außerdem gilt bezogen auf elektronische Systeme (siehe Chemikaliengesetz II 8.3):

„alle Datenänderungen müssen mit der sie ändernden Person verknüpft werden können, z. B. durch die Verwendung der mit Datum und Unterschrift versehenen (elektronischen) Unterschriften“.

Das OECD-Dokument gibt zusätzlich den Hinweis:

„Durch die Verwendung von mit Datum und Uhrzeit versehenen (elektronischen) Unterschriften soll es möglich sein, alle Datenänderungen auf die Personen zurückzuführen, die diese Änderungen vornahmen. Gründe für die Änderungen sind anzugeben“.

Die Art der elektronischen Unterschrift wird in beiden Passagen nicht explizit vorgegeben.

**Fazit: Im GLP-Bereich wird eine elektronische Unterschrift explizit zugelassen ohne Hinweis, welcher Art diese sein soll. Im Gegensatz zum GMP-Bereich wird hier gefordert, dass nicht nur die Abschlussberichte, sondern auch die Prüfpläne mit „datierter Unterschrift“ zu versehen sind.**

#### 2.2.4 GCP-Bereich

Für den GCP-Bereich gibt es hinsichtlich Unterschriften verschiedene Aspekte. In der ICH-Guideline Good Clinical Practice ist zwar nicht von „signature“ die Rede, wohl aber werden an verschiedenen Stellen ein „approved protocol“ oder eine „approval/favourable opinion“ gefordert.

Bei den deutschen Regularien sind die in Tab. 7 aufgeführten Passagen von Interesse, wobei Details den Tab. 8 und 9 im Anhang zu entnehmen sind.

Tab. 7: Hinweise auf Unterschriften/Unterzeichnungen im GCP-Bereich (Zusammenfassung der Tab. 8 und 9 im Anhang).

Quelle/§§	Absatz / Thema	Gefordert
AMG 1976 § 24 Sachverständigengutachten	Sachverständigengutachten Die Sachverständigen haben das Gutachten eigenhändig zu unterschreiben und dabei den Ort und das Datum der Erstellung des Gutachtens anzugeben.	Unterschrift
Good Clinical Practice-Verordnung Abschnitt 1/Allgemeine Vorschriften, § 3 Begriffsbestimmungen (2b)	Patienteneinwilligung nach Aufklärung zur Teilnahme an einer Studie	Unterschrift
Good Clinical Practice-Verordnung Abschnitt 3 /Genehmigung durch die Bundesoberbehörde und Bewertung durch die Ethik-Kommission, § 7 Antragstellung	Beantragung bei der zuständigen Ethik-Kommission und Antrag an die zuständige Bundesoberbehörde	Unterschrift

In der Praxis ist es unwahrscheinlich, dass Patienten- bzw. Probandeneinwilligungen elektronisch unterschrieben werden.

Werden Unterschriften, die nicht durch ein deutsches Gesetz gefordert sind (z. B. Clinical Development Plan, Data Management Plan, Investigator's Brochure, Clinical Study Protocol, Statistical Analysis Plan, Monitoring Manual) durch elektronische Signaturen ersetzt, wird empfohlen, den notwendigen Aufwand anhand einer Risikobetrachtung (siehe Kapitel 2.5) zu bestimmen und die Implementierung entsprechend Kapitel 3 und 4 vorzunehmen.

Analog den Bestimmungen im GMP-Bereich (s. o.) wird empfohlen, bei Bedarf folgende Richtlinien zu Rate zu ziehen:

- ICH-Guideline Good Clinical Practice
- 21 CFR Part 50 Protection of Human Subjects
- 21 CFR Part 54 Financial Disclosure by Clinical Investigators
- 21 CFR Part 56 Institutional Review Boards

**Fazit: Im GCP-Bereich treten keine zusätzlichen Forderungen auf. Die genannte Ausnahme (Patienten- bzw. Probandeneinwilligung) liegt außerhalb einer weiteren Betrachtungen dieser Empfehlung. Diese muss bei Bedarf individuell geregelt werden. Gutachten könnten zukünftig elektronisch unterschrieben werden, besonders wenn sie Teil einer elektronischen Zulassung sind. In diesem Fall sollte die Anwendung der elektronischen Signatur im Zusammenhang mit der elektronischen Zulassung geregelt werden.**

#### 2.2.5 Arzneimittelzulassung

Besonderes Augenmerk ist auf die elektronische Einreichung von Unterlagen zur Zulassung von Arzneimitteln zu legen. Es wird eine qualifizierte elektronische Signatur gefordert (siehe hierzu Tab. 8).

Tab. 8: Auszug aus der AMG-Einreichungsverordnung (AMG-EV).

§§	Absatz / Thema	
2 Pflicht zur Verwendung elektronischer Speichermedien für die Einreichung von Unterlagen	(2) Die verantwortende Person muss das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen.	„Qualifizierte elektronische Signatur“
5 Inkrafttreten	(2) § 2 Abs. 2 tritt in Kraft, sobald sichergestellt ist, dass die Voraussetzungen für eine qualifizierte elektronische Signatur nach dem Signaturgesetz bei der zuständigen Bundesoberbehörde gegeben sind. Das Bundesministerium für Gesundheit gibt den Tag des Inkrafttretens des § 2 Abs. 2 im Bundesgesetzblatt bekannt.	

**Fazit: Eine qualifizierte elektronische Signatur bei der elektronischen Zulassung von Arzneimitteln wird erforderlich werden. Zur Erläuterung des Begriffes „qualifizierte elektronische Signatur“ siehe Kapitel 2.3, „Juristische Betrachtung“.**

### 2.3 Juristische Betrachtung

Im Kapitel 2.2 wurde dargestellt, in welchen Fällen eine Unterschrift gefordert wird, und wo ein Kürzel oder ein Initial ausreichen. In diesem Kapitel wird beschrieben, wie im Falle einer geforderten Unterschrift diese in elektronischer Form zu leisten ist.

Zusätzlich zu den regulatorischen Anforderungen muss geprüft werden, ob Anforderungen an eine elektronische Signatur aus weiteren Rechtsfeldern zu berücksichtigen sind. Zu überprüfen sind hierbei das deutsche Signaturgesetz und der 21 CFR Part 11 der FDA.

#### 2.3.1 Deutsches Signaturgesetz (SigG)

Als nationale Umsetzung der EU-Richtlinie 1999/93/EG über elektronische Signaturen legt das deutsche Signaturgesetz in der aktuellen Überarbeitung von 2005 die Rahmenbedingungen für den Einsatz elektronischer Signaturen fest.

Zu Zweck und Anwendungsbereich des Signaturgesetzes heißt es in § 1:

- (1) Zweck des Gesetzes ist es, Rahmenbedingungen für elektronische Signaturen zu schaffen.
- (2) Soweit nicht bestimmte elektronische Signaturen durch Rechtsvorschrift vorgeschrieben sind, ist ihre Verwendung freigestellt.

In § 2 Begriffsbestimmungen wird nach drei Ebenen elektronischer Signaturen unterschieden:

- die einfache elektronische Signatur,
- die fortgeschrittene elektronische Signatur und
- die qualifizierte elektronische Signatur.

Dabei ist die **(einfache) elektronische Signatur** folgendermaßen definiert:

Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen.

Hier ist also noch keine Anforderung an die technische Umsetzung definiert. Anderes gilt für die **fortgeschrittene elektronische Signatur**. Hier fordert der Gesetzgeber, dass zusätzlich zur einfachen elektronischen Signatur folgende Anforderungen erfüllt werden:

- ... elektronischen Signaturen, die
- a) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
  - b) die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
  - c) mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
  - d) mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann, ...

Darüber hinaus erhöhte Anforderungen enthält die dritte Variante: Die qualifizierte **elektronische Signatur** erfüllt alle Anforderungen der fortgeschrittenen elektronischen Signatur und muss zusätzlich:

- a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und
- b) mit einer sicheren Signaturerstellungseinheit erzeugt werden.

**Qualifizierte Zertifikate** dürfen nur von Zertifizierungsdiensteanbietern erstellt werden. Die Anforderungen an diese Anbieter sind ebenfalls im Gesetz geregelt. Der Vollständigkeit halber sei erwähnt, dass sich Zertifizierungsdiensteanbieter freiwillig akkreditieren lassen können. Mittlerweile ist die überwiegende Mehrzahl der Zertifizierungsdiensteanbieter akkreditiert; die Akkreditierung ist indessen keine Voraussetzung für qualifizierte Zertifikate.

Eine **sichere Signaturerstellungseinheit** kann sowohl eine Software- als auch eine Hardware-Komponente sein, die bestimmte Anforderungen an die Speicherung des privaten Schlüssels erfüllt. Sie besteht in der Regel aus einer externen Eingabekomponente, wie zum Beispiel einer Chipkarte mit externem Chipkartenleser.

**Das Signaturgesetz schafft die Rahmenbedingungen für elektronische Signaturen, es fordert jedoch nicht den Einsatz elektronischer Signaturen (wie übrigens auch 21 CFR Part 11). Das Signaturgesetz fordert auch nicht, welche Signatur – die einfache elektronische, die fortgeschrittene elektronische oder die qualifizierte elektronische Signatur – verwendet werden soll. Vorgaben für die Verwendung bestimmter elektronischer Signaturen können sich aus anderen Rechtsvorschriften ergeben.**

In diesem Zusammenhang sei darauf hingewiesen, dass im Anschluss an das Signaturgesetz über das Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr das Bürgerliche Gesetzbuch (BGB) abgeändert wurde. Die elektronische Form der Unterschrift wurde als Alternative zur schriftlichen Form aufgenommen. In Buch 1 Titel 2 (Willenserklärung) wurde BGB § 126 (Schriftform) ergänzt. Dabei ist es wichtig, den Unterschied von Text- und Schriftform zu kennen:

BGB § 126 (1): Ist durch Gesetz schriftliche Form vorgeschrieben, so muss die Urkunde von dem Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigten Handzeichens unterzeichnet werden.

Dies bedeutet, dass stets eine Unterschrift erforderlich ist, wenn im Gesetz von Schriftform die Rede ist. Im Gegensatz dazu steht die Namensnennung in der Textform, die eine lesbare, dauerhafte, unterschriftslos gültige Dokumentationsform darstellt. Die Textform wird häufig für reine Mitteilungen verwendet. Das heißt, die Schriftform stellt somit die höherwertige Form dar.

Der Schriftform muss man sich bedienen, wenn sie als Form im Gesetz vorgeschrieben ist.

Hinweis: Die Formulierung „... ist schriftlich festzulegen ...“ bedeutet im juristischen Sinne nicht notwendigerweise, dass eine „Schriftform“ gemäß § 126 gefordert ist! Der Ausdruck „schriftliche Form“ jedoch ist identisch zu „Schriftform“.

Der entsprechend angepasste Inhalt von § 126 BGB lautet:

(3) Die schriftliche Form kann durch die elektronische Form ersetzt werden, wenn sich nicht aus dem Gesetz ein anderes ergibt.

Und im neu aufgenommenen § 126a BGB heißt es:

(1) Soll die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden, so muss der Aussteller der Erklärung dieser seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen.

(2) Bei einem Vertrag müssen die Parteien jeweils ein gleichlautendes Dokument in der in Absatz 1 bezeichneten Weise elektronisch signieren.

Hier findet sich erstmals die Forderung nach einer qualifizierten elektronischen Signatur.

Zusammengefasst bedeutet dies, dass in denjenigen Fällen, in denen der Gesetzgeber die Schriftform fordert und für die Dokumentation die elektronische Form gewählt wird, eine **qualifizierte elektronische Signatur** erforderlich ist (vgl. 2.2.5):

#### **Schriftform**

bestätigt durch eigenhändige Unterschrift

#### **Elektronische Form**

bestätigt durch qualifizierte elektronische Signatur

**In allen anderen Fällen bleibt die Verwendung der Art der Signatur freigestellt. Die Verwendung der qualifizierten elektronischen Signatur dient lediglich der Erlangung einer höheren Rechtssicherheit.**

Bleibt die Frage, ob es sich im pharmazeutischen Umfeld um Unterschriften handelt, die der Schriftform bedürfen.

**Fazit: Gemäß Signaturgesetz gibt es drei Unterscheidungen:**

- die einfache elektronische Signatur,
- die fortgeschrittene elektronische Signatur und
- die qualifizierte elektronische Signatur.

Die zuletzt aufgeführte Signatur ist stets dann anzuwenden, wenn laut Gesetz die **Schriftform** gefordert ist.

### 2.3.2 21 CFR Part 11

Für diejenigen Unternehmen, die den Anforderungen der US-amerikanischen FDA unterliegen, ergeben sich weitere juristische Anforderungen. Ähnlich wie im Signaturgesetz werden auch beim 21 CFR Part 11 keine elektronischen Signaturen gefordert. 21 CFR Part 11 enthält indessen Forderungen für den Fall, dass elektronische Signaturen umgesetzt werden. Wichtig ist hierbei der **Geltungsbereich**. 21 CFR Part 11 regelt lediglich den Umgang mit elektronischen Dokumenten und elektronischen Unterschriften, die in sog. „predicate rules“ (regulatorische Vorgaben) gefordert werden. Bei den „predicate rules“ handelt es sich im Wesentlichen um die GxP-Regeln der FDA (Anmerkung: Im 21 CFR Part 11 selbst wird der Begriff „predicate rules“ nicht verwendet, er findet sich jedoch in den Guidances zu 21 CFR Part 11).

cGMP:	21 CFR Parts 210/211
GLP:	21 CFR Part 58
GCP:	Klinische Studien: 21 CFR Parts 50, 54 und 56 Zulassung: 21 CFR Parts 310, 312 und 314
Medical Devices:	z. B. 21 CFR Part 820

Zum Beispiel wird in den cGMP-Regeln 21 CFR Parts 210/ 211 nur an sehr wenigen Stellen ein **Approval** verlangt, siehe hierzu Tab. 3 im Anhang.

Die Anforderungen gemäß 21 CFR Part 11 sind an vielen Stellen dargelegt und diskutiert. Nachfolgend eine Zusammenfassung der wichtigsten Kernelemente – die FDA unterscheidet zunächst grundsätzlich, ob es sich um offene oder geschlossene Systeme handelt:

Geschlossenes System	Umgebung, in der der Systemzugang durch diejenigen Personen kontrolliert wird, die für den Inhalt der elektronischen Dokumente verantwortlich sind.
Offenes System	Umgebung, in der der Systemzugang nicht durch diejenigen Personen kontrolliert wird, die für den Inhalt der elektronischen Dokumente verantwortlich sind.

Des Weiteren werden die folgenden Unterschriftstypen definiert:

Electronic signature	Mittels Computertechnik verarbeitetes Symbol oder Symbolserien, die von einer Person ausgeführt, angewendet oder autorisiert wurde, um als rechtsgültiges verbindliches Äquivalent zur handschriftlichen Unterschrift zu gelten.
Digital signature	Electronic signature basierend auf kryptografischen Methoden der Urheberauthentisierung. Zur Verschlüsselung werden jeweils ein Regel- und ein Parametersatz verwendet, um die Urheberidentität und die Datenintegrität zu verifizieren.
Biometrics	Methode zum Nachweis der Identität einer Person, basierend auf physischen Eigenschaften oder wiederholbaren Handlungen, die die Person eindeutig kennzeichnen und messbar sind.

Bei der „digital signature“ wird – im Gegensatz zur qualifizierten elektronischen Signatur – die Inanspruchnahme eines zertifizierten Trust Centers nicht verlangt.

Die Hauptforderungen an elektronische Signaturen sind:

Die elektronische Signatur muss mindestens drei Komponenten enthalten:

- Name des Unterzeichnenden (in Druckbuchstaben)
- Datum und Zeit der Signaturerstellung
- die Bedeutung der Unterschrift

Die elektronische Signatur muss mit dem elektronischen Dokument in einer Weise verknüpft sein, dass die elektronische Signatur nicht ausgeschnitten, kopiert oder auf andere Art transferiert werden kann, um elektronische Dokumente zu verfälschen.

Für die Unterschriftstypen sind unterschiedliche Anforderungen definiert:

Nicht-biometrische Unterschrift:

- Zwei verschiedene Komponenten zur Identifikation (Benutzer-ID und Passwort).
- Bei fortlaufenden, nicht unterbrochenen Sitzungen genügt das Passwort.
- Bei unterbrochenen Sitzungen sind beide Komponenten einzugeben.
- Komponenten müssen eindeutig und personengebunden sein.
- Entsprechende Sicherheitsvorkehrungen müssen existieren, damit keine einzelne Person sich beide Identifikations-Komponenten einer anderen Person beschaffen kann.

Biometrische Unterschrift:

- Gestaltung in einer Form, die nur durch deren Eigentümer verwendet werden kann (dies muss durch eine Validierung nachgewiesen werden).

Nur für offene Systeme wird der Einsatz digitaler Signaturen gefordert.

**Hinweis:** Bereits die fortgeschrittene elektronische Signatur nach dem Signaturgesetz erfüllt die Anforderungen einer „**digital signature**“ nach 21 CFR Part 11. Die „electronic signature“ ist aus technischer Sicht vergleichbar mit der einfachen Signatur nach dem Signaturgesetz.

21 CFR Part 11 spezifiziert die technische Umsetzung der elektronischen Signatur nicht so detailliert wie das deutsche Signaturgesetz. Er regelt jedoch im Detail die Rahmenbedingungen beim Einsatz elektronischer Signaturen wie etwa:

- Systemvalidierung
- Möglichkeit der Erstellung genauer und vollständiger Kopien in elektronischer Form und Papierform
- Erhalt und Pflege der Dokumente über die gesamte Lebenszeit
- Zugangskontrollsystem
- Computergenerierte Audit Trails
- Erzwingen eines vorgegebenen Arbeitsablaufes
- Überprüfung von Eingabegeräten
- Anforderungen an das Personal (Schulungen, Verantwortung bei Nutzung elektronischer Signaturen etc.)
- Kontrollen der Systemdokumentation

#### 2.4 AMWHV und AMG: Auswirkung der juristischen Betrachtungen auf regulatorische Anforderungen in den Bereichen GMP, GLP, GCP

##### GMP

Wie bereits im Kapitel 2.2 beschrieben, wird durch die Formulierung in der AMWHV §10, Abs. 2 festgelegt, dass beim Einsatz automatischer Datenverarbeitung statt der eigenhändigen Unterschrift die Wiedergabe des Namens des Verantwortlichen ausreicht, wenn

„... in geeigneter Weise sichergestellt ist, dass nur befugte Personen die Bestätigung über die ordnungsgemäße Ausführung der jeweiligen Tätigkeiten vornehmen können“.

Somit ergibt sich im Bereich der AMWHV keine juristische Forderung nach Verwendung einer qualifizierten elektronischen Signatur.

**Fazit: Die Anforderungen des Signaturgesetzes können im Geltungsbereich von AMWHV und AMG eine Hilfestellung geben und verschiedene Sicherheitsstufen von Signaturen vorgeben. Eine Verpflichtung zur Anwendung einer der dort definierten Signatur (einfache, fortgeschrittene oder qualifizierte elektronische Signatur) ist aus der AMWHV nicht ableitbar.**

Die einzige im AMG geforderte Unterschrift betrifft das Sachverständigengutachten § 24. Diese wird als Schriftform interpretiert (vgl. 2.2.4).

Die im pharmazeutischen Produktionsumfeld verwendeten Unterschriften und Bestätigungen sind hier nicht erwähnt.

##### GLP

Ausgehend von der oben beschriebenen Gesetzeslage bedeutet das für den GLP-Bereich:

In einigen Fällen (siehe hierzu auch Kapitel 2.2.3 bzw. Tab. 4 bis 7 im Anhang) wird explizit die Unterschrift statt des Kennzeichens gefordert. Juristisch könnte diskutiert werden, ob eine qualifizierte Signatur zu verwenden ist. Im Rahmen einer Risikoanalyse wäre zu prüfen, welche technische Umsetzung sinnvoll und erforderlich ist.

##### GCP

Aus den Erläuterungen im Kapitel 2.2.4 ergibt sich speziell für den Außenbereich eindeutig, dass für die Themen „Patienteneinverständniserklärung“ und „Sachverständigengutachten zur Zulassung“ eine einfache elektronische Signatur nicht ausreichend sein kann.

##### Verordnungen zum AMG

Wie bereits erwähnt, soll auf einzelne Verordnungen zum AMG nicht eingegangen werden. Es ist jedoch darauf hinzuweisen, dass z. T. sehr präzise Anforderungen gestellt werden. In der Verordnung über die Verschreibungspflicht von Arzneimitteln (Arzneimittelverschreibungsverordnung – AMVV) ist explizit die eigenhändige Unterschrift der verschreibenden Person oder, bei Verschreibungen in elektronischer Form, deren qualifizierte elektronische Signatur nach dem Signaturgesetz gefordert. Ist die Anforderung eines Arzneimittels für ein Krankenhaus bestimmt, in dem zur Übermittlung derselben ein System zur Datenübertragung vorhanden ist, das die Anforderung durch eine befugte verschreibende Person sicherstellt, so genügt anstelle der eigenhändigen Unterschrift nach § 2, Absatz 1, Nr. 10 der AMVV die Namens-

wiedergabe der verschreibenden Person oder – bei Anforderungen in elektronischer Form – ein geeignetes elektronisches Identifikationsverfahren.

Ein weiteres Beispiel ist die Verordnung über die Einreichung von Unterlagen in Verfahren für die Zulassung und Verlängerung der Zulassung von Arzneimitteln (AMG-Einreichungsverordnung – AMG-EV). Wie im Kapitel 2.2.5 bereits erwähnt, ist die elektronische Einreichung von Unterlagen vorgeschrieben, sobald sichergestellt ist, dass die Voraussetzungen für eine qualifizierte elektronische Signatur nach dem Signaturgesetz bei der zuständigen Bundesoberbehörde gegeben sind.

In denjenigen Fällen, in denen der Gesetzgeber eine qualifizierte elektronische Signatur erwartet, ist dies in der Regel auch kenntlich gemacht.

## 2.5 Risikobasierter Ansatz

Bei der Auswahl geeigneter Signaturverfahren und der Festlegung der begleitenden Maßnahmen ist es naheliegend, einen risikobasierten Ansatz zu wählen.

Auch aus den Gesetzestexten ist oftmals abzulesen, wo der Gesetzgeber selbst ein höheres oder niedrigeres Risiko sieht. In der neuen AMWHV z. B. werden bezogen auf Herstellvorschriften und Prüfvorgaben nur „schriftliche Vorgaben“ verlangt, wohingegen beim Herstellprotokoll und Prüfprotokoll explizit Datum und Unterschrift gefordert werden.

Liegt keine direkte gesetzliche Anforderung nach einem bestimmten Unterschriftentyp vor, so ist für die Entscheidung, welcher Form der elektronischen Signatur der Vorzug zu geben ist, die Identifikation der mit dem Prozess der Unterzeichnung verbundenen pharmazeutischen Risiken ausschlaggebend.

Bei der Risikobewertung und Auswahl der elektronischen Signatur kann mit einbezogen werden, dass es sich im pharmazeutischen Umfeld in der Regel um Unterschriften im Innenverhältnis handelt. Es besteht daher eine klare Abgrenzung zu Unterschriften im Geschäftsverhältnis, mit denen Verträge zwischen verschiedenen Parteien geschlossen werden.

Die FDA vollzieht im 21 CFR Part 11 mit der Unterscheidung in geschlossene und offene Systeme bereits einen risikobasierten Ansatz: In offenen Systemen ist die Manipulationsgefahr deutlich erhöht; daher werden entsprechende erweiterte Maßnahmen gefordert. Auch für Systeme, bei denen keine FDA-Anforderungen zu erfüllen sind, kann dies für die eigene Risikobetrachtung mit berücksichtigt werden.

Bei der Auswahl der Signatur sollte auch die notwendige Aufbewahrungsdauer der signierten Dokumentation berücksichtigt werden. Bei Signaturen mit Zertifikaten sind oftmals die Gültigkeitsdauern der Zertifikate kürzer als typische Aufbewahrungszeiten.

Im folgenden werden einige Risiken im Zusammenhang mit elektronischen Signaturen beschrieben und Möglichkeiten der Risikominimierung aufgezeigt. Es ist jedoch nicht beabsichtigt, eine Skala zunehmender Risikoprioritäten zu entwickeln und diese den wachsenden strengeren Unterschriftenformen zuzuordnen. Dies wäre eine zu starre Darstellung, die im jeweils konkreten Fall ohne Berücksichtigung der gegebenen System- und Ablaufbesonderheiten zu allgemein wäre und lediglich zu einem schematischen Missbrauch verleiten würde.

### Bewusste Fälschung von Daten

Eine bewusste Fälschung von unterzeichneten Daten liegt vor, wenn eine Person absichtlich diese Daten oder die zugehörige Unterschriftskennung manipuliert. Bei Manipulationen ist zu unterscheiden nach:

- Unternehmensinterne Manipulationen – Manipulationen, die z. B. durch einen Mitarbeiter des Unternehmens, in dem die Daten anfallen, versucht werden, und
- Manipulationen von außen – Manipulationen durch Personen, die hiermit dem Unternehmen schaden wollen. Voraussetzung dabei ist, dass die Daten das Unternehmen verlassen oder aber ein Zugriff von außen möglich ist.

Unternehmensinterne Manipulationen können und sollen durch ein angemessenes Rechtekonzept verhindert werden. Darüber hinaus sollte ein Audit Trail des Systems Datenänderungen mitprotokollieren. Es ist empfehlenswert, die Zugriffsmöglichkeit von Administratoren zu hinterfragen und ggf. einzuschränken. Manipulationen durch Administratoren können in vielen Fällen technisch durch eine aussagefähige Auswertung der Log-Dateien erkannt werden.

Hier, wie auch in anderen Fällen gilt, dass nicht alleine die technische Natur der Signatur, wie etwa fortgeschrittene oder qualifizierte Signatur, das Auswahlkriterium sein sollte, sondern die Kombination aus technischer Umsetzung, organisatorischem Umfeld und Einsatzzweck. Der Fokus sollte auf der Auswahl geeigneter Mechanismen und einer professionellen Umsetzung liegen, die durch Tests und Dokumentation nachgewiesen werden.

Manipulationen von Daten, die das Unternehmen verlassen, sind schwieriger zu verhindern. Einer Risikobetrachtung vorangestellt werden sollte eine Analyse der Netze für den Datenaustausch. Ein erhöhtes Risiko ist dann gegeben, wenn die Daten

öffentlich leicht zugänglich sind. Die Absicherung mit einer digitalen Signatur verhindert hier den Missbrauch. Ist zusätzlich zu befürchten, dass auch die öffentlichen Schlüssel oder beigefügten Informationen manipuliert werden könnten, ist der Einsatz einer qualifizierten elektronischen Signatur empfehlenswert.

Bei der Auswahl der Signatur sollte stets der gesamte Prozess betrachtet und anschließend das Gesamtrisiko beleuchtet werden. So ist zum Beispiel denkbar, dass beim Einsatz einer Signaturlösung in einem lokalen Netzwerk durch die bei der qualifizierten elektronischen Signatur geforderte Notwendigkeit der Einbeziehung eines Trust Centers eine Verbindung nach außen hergestellt werden muss. Dies kann das Gesamtrisiko gegenüber einer lokal einsetzbaren Signatur erhöhen.

### **Versehentliche Verfälschung von Daten im System**

Die versehentliche Verfälschung von Daten stellt für Datenbestände, die in Papierform anfallen, im allgemeinen kein hohes Risiko dar. Anders verhält es sich bei DV-Systemen, für die in der Regel ein Workflow existiert mit einer Erstellungsphase, einer Prüfphase mit anschließender Unterzeichnung und einer Phase, in der das Dokument oder die Datei gültig ist.

Beispiele sind Labordaten, die in Excel-Tabellen eingetragen werden oder Dokumente wie SOPs, die in einem DMS erstellt werden. Während des Erstellungsprozesses sind versehentliche Änderungen durchaus möglich, da die Bearbeitung der Daten zum Erstellungsprozess gehört.

Das Risiko einer Änderung in dieser Phase ist insofern relevant, weil eine versehentliche Änderung nicht ohne weiteres erkannt wird und dazu führen kann, dass Datenbestände unterzeichnet werden, die nicht den Inhalt haben, den der Unterzeichner erwartet.

Risikominimierende Maßnahmen hierbei sind:

- Beschränkung der Änderungserlaubnis auf einen eingeschränkten Nutzerkreis über ein Berechtigungskonzept.
- Definition einer Prüfphase vor dem Signieren, ab deren Beginn das Dokument vor Änderungen geschützt ist mit dem Zweck, Änderungen während der Prüf- und Unterschriftsphase zu verhindern.
- Schulungsmaßnahmen.

Zusammengefasst bedeutet dies, dass das System-Design versehentliche Änderungen verhindern oder das Risiko hierfür minimieren muss. Die Anwenderschulung wird ergänzend eingesetzt.

Die versehentliche Änderung nach dem Unterschreiben ist schwerwiegender und hat andere Ursachen. Hier muss die Kombination von technischen und organisatorischen Maßnahmen die Fehlerquellen ausschalten; dazu gehören: Berechtigungskonzept, Schreibschutz, ggf. Auswahl geeigneter Archivierungsmethoden etc. Näheres hierzu siehe auch in den Kapiteln 3 und 4.

Ein Beispiel aus der Praxis:

Ein im Labor zu erstellender Prüfplan beschreibt eine Reihe von Prüfungen und ist vor Beginn der Laborarbeiten zu unterzeichnen. Sollten die einzutragenden Informationen umfangreich sind, sind mehrere Masken für die Umsetzung erforderlich.

Vor der Unterzeichnung sind Änderungen ohne weiteres möglich und die Berechtigung dazu für einen befugten Personenkreis beabsichtigt. Die Gefahr einer versehentlichen Änderung ist dadurch gegeben, dass die Informationen im System selbst nicht direkt erfasst werden können und somit auch nicht auf Anhieb erkannt werden. Eine Abhilfe könnte durch geeignete Ausdrücke geleistet werden. Die Nutzerschulung könnte empfehlen, dass vor der elektronischen Unterzeichnung die Richtigkeit der Daten in einem Ausdruck sichergestellt wird. Auch eine Absicherung dieser Überprüfung durch eine Arbeitsanweisung kann sinnvoll sein.

Nach der Unterzeichnung dagegen wird man im allgemeinen nur mit einem Audit Trail und der Aufforderung einer erneuten elektronischen Signatur die Daten ändern können. Ein Versehen durch die gewöhnlichen Systemanwender ist daher kaum möglich. Es ist auch zu überprüfen, ob Daten versehentlich durch Personen geändert werden können, die weitgehende Systemrechte besitzen, z. B. Administratoren. Es ist also wichtig, das Berechtigungskonzept sinnvoll zu konzipieren und diese weitgehenden Systemrechte kritisch zu hinterfragen.

### **Versehentliche Datenverfälschung bei Hybrid-Systemen**

Entscheidet man sich gegen eine elektronische Signatur und erstellt stattdessen Ausdrücke und unterschreibt diese, besteht das Risiko, dass die elektronischen Daten, die dem unterzeichneten Datenbestand zugrundeliegen, in abgeänderter Form für andere Zwecke weiter verwendet werden. Das rechtsgültige Original ist das unterschriebene Papierdokument, und es ist sicherzustellen, dass es keine Abweichungen zwischen Papier und elektronischen Daten gibt. Ist aber der unterzeichnete Datenbestand umfangreich, ist die Sicherstellung dieser Kongruenz gefährdet. Hier kann eine Unterschriftslösung, die auf einem technisch weniger aufwendigen Sicherheitsstandard ansetzt, für den Ablauf insgesamt sicherer sein als die Nutzung einer Hybrid-Lösung.

### „Initial“ oder „Signature“

In den Regularien werden an verschiedenen Stellen die Begriffe „Initial“ oder „Kürzel“ oder „Signature“ verwendet.

Es handelt sich dabei um zwei Aktivitäten mit unterschiedlicher Zielsetzung und unterschiedlichem Risiko für den Gesamtprozess. Das Kürzel wird in denjenigen Fällen eingesetzt, bei denen die Durchführung einer Aktion bestätigt wird und diese Aktion einem Anwender zugeordnet werden soll. Sie hat den Charakter eines Logbuch-Eintrages und kann sehr gut über einen Audit Trail abgebildet werden.

Eine Signature bestätigt die Durchführung eines Prüf- oder Kontrollschrittes. Sie hat einen höheren Stellenwert.

Anders als im GAMP-Good Practice Guide: A Risk-Based Approach to Compliant Electronic Records and Signatures wird hier also klar zwischen Initial (Kürzel) und Signature (Unterschrift) unterschieden und festgestellt, dass für Initials die Anforderungen an elektronische Signaturen nicht erfüllt sein müssen.

In diesem Sinne könnte zum Beispiel auch ein qualifizierter Audit Trail, in dem Datum und Uhrzeit sowie der ausführende Benutzer eindeutig aufgeführt werden, ausreichend sein.

Jedes Unternehmen sollte grundsätzlich individuell entscheiden und festlegen, wie diese Begriffe intern zu definieren und zu bewerten sind, ferner an welchen Stellen bei der Forderung eines „Initial“ trotzdem aufgrund der Risikobetrachtung die Anforderungen an elektronische Signaturen erfüllt werden müssen.

### Technik und Risiken

In Tab. 9 „Techniken und Risiken“ ist zusammengefasst, welche der Signaturarten die unterschiedlichen technischen Anforderungen aus 21 CFR Part 11 erfüllen können. Die in dieser tabellarischen Darstellung nach rechts zunehmenden Anforderungen an elektronische Signaturen sind in einer Kopfzeile aufgelistet, während in der ersten Spalte mögliche technische Realisierungen gezeigt werden. Auf diese Weise kann in der Kombination aus Kopfzeile und erster Spalte z. B. abgelesen werden, dass etwa eine Signatur über die Angabe von Nutzer-ID und Passwort die Anforderungen des 21 CFR Part 11 an geschlossene Systeme erfüllt und gleichzeitig auch eine manipulationssichere Verknüpfung von Signatur und Dokument gewähren kann, wenn die konkrete technische Umsetzung dies sicherstellt.

Ein Audit Trail kann als Zusatz verwendet werden, um sämtliche Änderungen an schon bestätigten Datensätzen zu verfolgen. Als alleinige Maßnahme ist er in denjenigen Fällen einsetzbar, in denen in der Papierform eine Bestätigung mit Kürzel verlangt wird. Zum Signieren indessen ist er nicht ausreichend, da der Akt der willentlichen Erklärung fehlt.

Signaturen auf der Basis einer unternehmensintern geführten Public-Key-Infrastruktur (PKI) können als vollständige Unterschrift eingesetzt werden. Voraussetzung ist, dass sie allen Anforderungen, die in den Spalten A bis E aufgeführt sind, entsprechen. Sie können auch die Anforderungen des 21 CFR Part 11 für offene Systeme erfüllen, nicht jedoch die Anforderungen der qualifizierten elektronischen Signatur.

Digitale Signaturen mit Zertifikat erfüllen insgesamt alle Anforderungen, wobei aktiv dafür gesorgt werden muss, dass die Anforderungen, die in den Spalten A bis E definiert sind, erfüllt werden.

Um die Anforderungen von 21 CFR Part 11 abzudecken, genügt es nicht, eine der aufgeführten technischen Signaturarten zu implementieren, es müssen zusätzliche organisatorische Maßnahmen umgesetzt werden. So können zwar sowohl die fortgeschrittene als auch die qualifizierte Signatur die Anforderungen für offene Systeme erfüllen, ohne weitere Maßnahmen indessen erfüllt die technisch anspruchsvolle qualifizierte Signatur weder die Anforderungen an offene noch an geschlossene Systeme.

So ist auch zu berücksichtigen, dass zusätzliche organisatorische Maßnahmen und Validierungsaktivitäten erforderlich sind, um elektronische Signaturen im pharmazeutischen Umfeld einzusetzen. Die Validierung des Systems und der Betrieb in einer qualifizierten Umgebung (IT-Infrastruktur) sind hierbei zu beachten. Details sind in den Kapiteln 3 und 4 zu finden.

Bei international agierenden Unternehmen kann der Einsatz von qualifizierten Signaturen zu Problemen führen. Außerhalb Deutschlands ist die Forderung nach der Einbindung von Trust Centern nur selten gegeben, und sie stehen somit auch nicht zur Verfügung. Auch die Nutzung deutscher Trust Center durch im Ausland ansässige Personen ist nicht ohne weiteres möglich. Es bleibt daher oft nur die Möglichkeit, auf papierbasierte Dokumente auszuweichen – was einen technologischen Rückschritt bedeuten würde – oder andere pragmatische Lösungen anzustreben. Eine solche pragmatische Lösung könnte z. B. sein, Teilberichte mit einer nicht-qualifizierten elektronischen Signatur zu unterzeichnen und einen zusammenfassenden Bericht mit der qualifizierten elektronischen Signatur zu versehen. Letzteres hätte die Funktion eines signierten Deckblattes.

Tab. 9: Techniken und Risiken der elektronischen Signatur.

Bedingungen, die die Signatur erfüllt →	A	B	C	D	E	F	G	H
Art der Signatur ↓	Weist mindestens zwei Identifikationskomponenten auf (Ausnahme: biometrische Signatur)	Gibt den Namen des Signierenden an	Gibt Datum und Zeitpunkt der Ausführung der Signatur an	Wird vom Anwender auf seine Anforderung hin geleistet	Gibt die Bedeutung der Signatur an (z.B. Prüfung, Freigabe, Verantwortlichkeit, Urhebererschaft)	Manipulations-sichere Verknüpfung von Signatur und Dokument	Erfüllt die Anforderungen von 21 CFR Part 11	Erfüllt die Anforderungen an die qualifizierte Signatur
Manueller Eintrag des Anwendernamens (keine systemgestützte Authentifizierung)	Nein	Ja	Möglich	Ja	Möglich	Nein	Nein	Nein
Audit Trail (Metainformation als Logbuch eines Datenobjekts)	Nein	Zuordnung zum Namen ist möglich	Ja	Nein	Ja	Abhängig von technischer Lösung	Nein	Nein
Nutzer ID & PW	Ja	Möglich	Möglich	Ja	Möglich	Abhängig von technischer Lösung	Für geschlossenes System	Nein
Nutzer ID & PW+Verschlüsselung gemeinsam mit Daten (z. B. PKCS#7)	Ja	Möglich	Möglich	Ja	Möglich	Ja	Auch für offenes System	Nein
Biometrische Signatur	Anforderung erfüllt	Möglich	Möglich	Ja	Möglich	Abhängig von technischer Lösung	Für geschlossenes System	Nein
Signatur mit PKI-Struktur (Internes Zertifikat)	Möglich, auch biometrische Lösungen	Möglich	Möglich	Ja	Möglich	Ja	Auch für offenes System	Nein
Signatur mit PKI-Struktur und externes Zertifikat	Möglich, auch biometrische Lösungen	Möglich	Möglich	Ja	Möglich	Ja	Auch für offenes System	Ja

**2.6 Schlussfolgerung**

Für die Sicherstellung der Datenintegrität ist es wichtig, das gesamte Umfeld des Systems und seiner Nutzung einzubeziehen. Nachfolgende zusammenfassende Darstellung zeigt noch einmal die Einflüsse und Abhängigkeiten auf den Prozess sowie die Bedeutung der elektronischen Signatur, welche dann wiederum die Vorgaben für die Anwendung und die Hard- und Software bilden (Abb. 1).

1. Die technischen Anforderungen bzgl. der Art der elektronischen Signaturen ergeben sich aus dem Signaturgesetz und 21 CFR Part 11.
2. Die regulatorischen Anforderungen definieren, ob formal eine „Schriftform“ gefordert ist oder eine Textform ausreicht.
3. Es muss definiert werden, ob eine „Bestätigung von Daten“ oder aber eine „regulatorische Unterschrift“ elektronisch geleistet werden soll.
4. Nach Überprüfung dieser drei Einflüsse auf den Prozess sollte in der Risikobewertung der Prozessablauf zusammen mit der Bedeutung der Unterschrift betrachtet werden.
5. Daraus resultieren letztlich die Vorgaben für die Anwendung und das System.

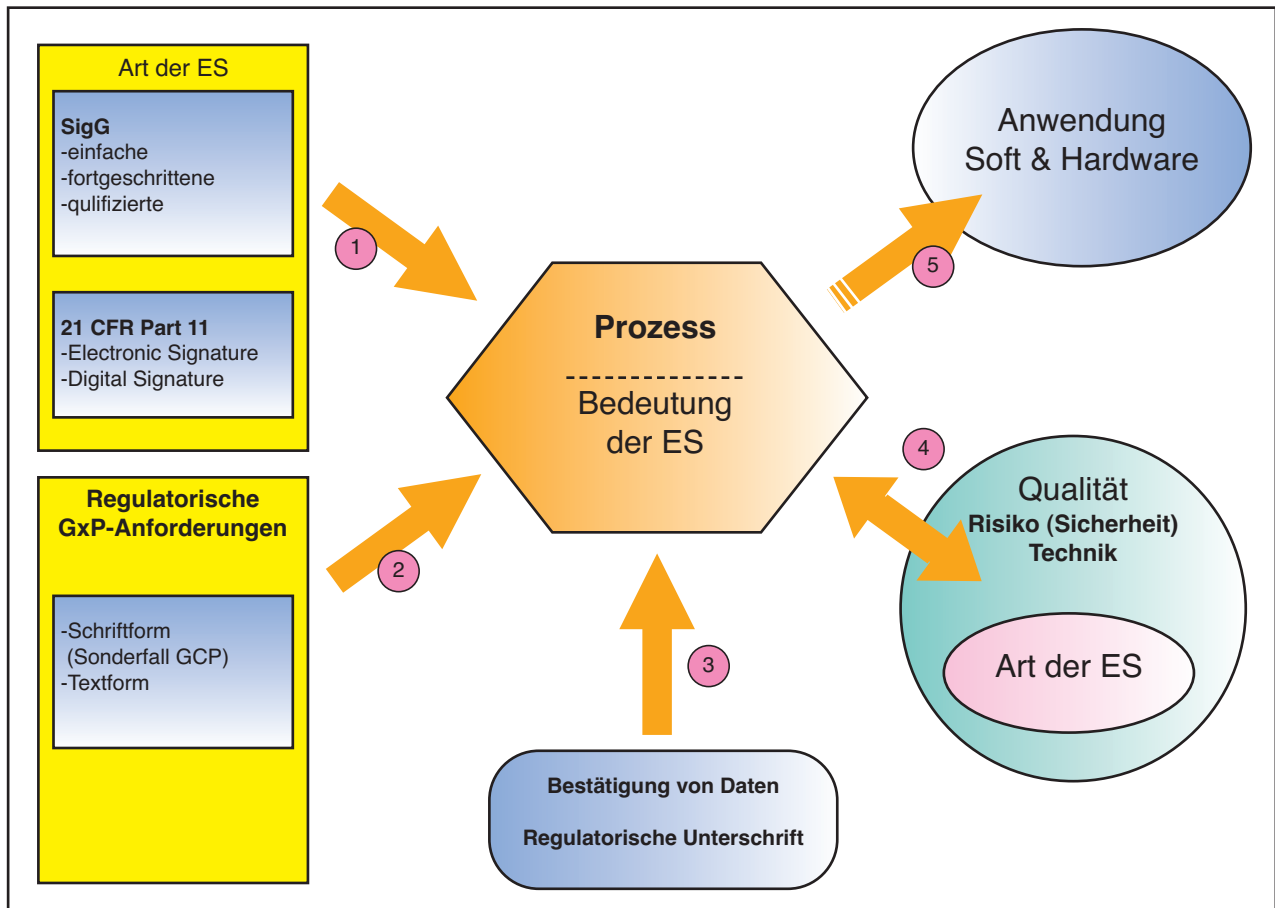


Abb. 1: Elektronische Signatur im regulierten Prozessumfeld.

Generell kann gesagt werden, dass keine direkte Beziehung zwischen der Art der Unterschrift und den Vor- bzw. Nachteilen im Prozess besteht. Technisch weniger komplexe Lösungen – eingebettet in das geeignete organisatorische Umfeld – können bereits für viele Systeme ausreichenden Schutz bieten. In einigen Fällen allerdings kann aufgrund von Risikoerwägungen eine komplexe Lösung erforderlich sein, wobei aus der Komplexität wieder neue Risiken entstehen können. Eine sorgfältige Bewertung, welche Risiken vorliegen und wie man sie minimieren kann, ist entscheidend, um im jeweiligen Fall angemessen vorgehen zu können.

### 3 Organisation

Beim Einsatz von elektronischen Signaturen spielt das organisatorische Umfeld eine wesentliche Rolle. Organisatorische Anforderungen müssen vor dem Produktivstart des Systems erfüllt und die entsprechenden Maßnahmen etabliert sein. Sie sind abhängig von der Art der elektronischen Signatur und der technischen Umsetzung.

Für die besonderen Anforderungen, die sich aus 21 CFR Part 11 ergeben, siehe Kapitel 2.3.2.

Mit zunehmendem Sicherheitsgrad (fortgeschrittene oder qualifizierte elektronische Signatur gemäß Signaturgesetz) sind die organisatorischen Rahmenbedingungen entsprechend anzupassen bzw. zu ergänzen. Einer organisatorischen Regelung bedürfen:

- Rechtsverbindlichkeit der Unterschrift
- Manipulationsschutz
- Betrieb

#### 3.1 Rechtsverbindlichkeit

##### 3.1.1 Rechtsverbindlichkeit im Verhältnis Mitarbeiter – Firma

Es wird empfohlen, dass jeder Mitarbeiter, der eine elektronische Signatur leisten soll, vorab eine Erklärung zur Äquivalenz von elektronischer und handgeschriebener Unterschrift gegenzeichnet – nach 21 CFR Part 11 ist dies sogar erforderlich – als Teil der Umsetzung der Forderungen § 11.10 (i) + (j) sowie § 11.100 (c) (2) – Schulungsnachweis. Diese Erklärung sollte folgende Informationen enthalten:

- Hinweis zur Rechtsverbindlichkeit der elektronischen Unterschrift und Umgang mit Passwörtern und Zertifikaten
- Namen im Klartext
- Ggf. Nutzer-ID
- Kenntnisnahme des Mitarbeiters, bestätigt per handschriftlicher Unterschrift

Auf diese Weise wird die Äquivalenz zwischen handschriftlicher und elektronischer Unterschrift durch den Nutzer bestätigt.

Gleichzeitig erkennt dieser den rechtsverbindlichen Charakter an.

Diese Klarstellung liegt auch im Interesse des Mitarbeiters.

In Abb. 2 wird beispielhaft ein solches Formular wiedergegeben.

<b>&lt;Firma&gt;</b>		<b>&lt;Abteilung&gt;</b>
<p>Hiermit erkenne ich die elektronische Unterschrift in den bei &lt;..&gt; verwendeten Systemen an. Ich bin mir bewusst, dass diese den gleichen rechtsverbindlichen Charakter besitzt wie meine handschriftliche Unterschrift. Ferner bestätige ich, dass ich das/die Passwort(e) zum Leisten der elektronischen Unterschrift nicht weitergebe.</p>		
<b>user ID</b>	<b>Name</b>	<b>Unterschrift</b>
<p>Hiermit bestätige ich die Authentizität der unterschreibenden Mitarbeiter:</p> <p>Datum, Unterschrift &lt;Vorgesetzter&gt;</p>		

Abb. 2: Formular für die Rechtsverbindlichkeit.

### 3.1.2 Rechtsverbindlichkeit im Verhältnis Firma – Behörde (hier: FDA)

Eine Besonderheit ergibt sich für diejenigen Organisationen, welche die Anforderungen des 21 CFR Part 11 erfüllen müssen.

Die Anforderung gemäß § 11.100 (c) (1) nach einem Zertifizierungsschreiben an die FDA kann durch ein formloses Schreiben erfüllt werden. Ein Beispiel hierzu gibt Abb. 3.

To whom it may concern:

In reference to electronic signatures pursuant to Title 21 Code of Federal Regulations, Part 11.100 (c), this letter is to certify that all electronic signatures executed to electronic records in <company>, used on or after <date> pertaining to records relevant to Federal Food and Drug Administration regulations, are intended to be the legally binding equivalent of traditional hand written signatures

Abb. 3: Zertifizierungsschreiben an die FDA.

Die Benachrichtigung der FDA ist nur erforderlich, wenn nach „predicate rules“ geforderte Unterschriften (siehe Kapitel 2.3.2) durch elektronische Signaturen ersetzt werden.

Das bedeutet nicht, dass ab diesem Zeitpunkt die elektronische Signatur verwendet werden muss, sondern lediglich, dass diese als gleichberechtigt zur handschriftlichen Unterschrift angesehen wird und als solche eingesetzt werden kann. Letztendlich wird in den Nutzeranforderungen festgelegt, ob überhaupt und in welcher Form eine rechtsverbindliche Unterschrift erfolgt (elektronisch oder handschriftlich auf einem Ausdruck).

### 3.2 Manipulationsschutz

Das System, in dem die elektronischen Signaturen eingesetzt werden, muss über einen ausreichenden Manipulationsschutz verfügen. Manipulationen an signierten Daten (z. B. signierte Dokumente) müssen verhindert werden bzw. klar erkennbar sein. Neben den technischen Maßnahmen zum Manipulationsschutz (siehe Kapitel 4.1.2) sind auch organisatorische Maßnahmen zu treffen. Dazu gehören das Berechtigungskonzept für die Ausführung der Signatur und das Berechtigungskonzept für die Nutzung des Systems. Auch das Thema Administratorenrechte muss adäquat reguliert werden.

### 3.3 Regelungen zum Betrieb

Um den gesetzlichen und vom Prozess vorgegebenen Anforderungen gerecht zu werden, sind verbindliche Regelungen zum Betrieb des Systems zu etablieren. Details hierzu siehe im Kapitel 4 „Anforderungen an die Validierung“.

## 4 Anforderungen an die Validierung

Nachfolgend wird erläutert, in welchen Phasen des Validierungsablaufs ergänzende Aktionen bzgl. der Einführung von elektronischen Signaturen erforderlich und welche Mindestanforderungen zu erfüllen sind. Dies bezieht sich im allgemeinen nicht nur auf das System allein, sondern auch den Aspekt einer qualifizierten IT-Infrastruktur, in die das System eingebettet sein muss.

### 4.1 User Requirements, Spezifikation, Design, Risikoanalyse

#### 4.1.1 Allgemeines

Beim Einsatz elektronischer Signaturen sollten in den User Requirements folgende Aspekte behandelt werden (siehe auch Tab. 10):

- Beschreibung, für welche Prozess-Schritte eine Unterschrift erfolgt
- Festlegung des Charakters der Unterschrift (rechtsverbindlich, interne Bestätigung ...)
- Form der Unterschrift (elektronisch oder handschriftlich auf einem Ausdruck)
- Mindestanforderungen an die Signatur
  - Mindestens zwei Identifikationskomponenten (Ausnahme biometrische Signatur)
  - Name des Signierenden
  - Datum und Zeitpunkt der Ausführung der Signatur
  - Anlass/Bedeutung der Signatur (z. B. Prüfung, Freigabe, Verantwortlichkeit, Urheberschaft)
  - Manipulationssichere Verknüpfung von Signatur und zugehörigen Daten
  - Bei Hybrid-Systemen Angabe von Datum und Zeitpunkt des Ausdruckes sowie Referenz zu den elektronischen Daten
  - Gültigkeitsdauer der Signatur im Verhältnis zu den einzuhaltenden Aufbewahrungsfristen
- Definition des Authentifizierungsverfahrens (inkl. Sicherstellung der Eindeutigkeit)
- Möglichkeit des Monitorings fehlgeschlagener Signaturversuche
- Möglichkeit des automatisierten Entzuges von Rechten
- Audit Trail/Funktionalität
  - Ein Mitarbeiter muss sich sicher sein können, dass ein von ihm signierter Datensatz nachträglich nicht mehr geändert werden kann, ohne dass transparent wird, dass (und welche) Änderungen vorgenommen wurden.
  - Es ist zu dokumentieren, wer wann was geändert hat.
  - Im System muss optisch erkennbar sein, dass eine Änderung von freigegebenen Daten stattgefunden hat.
  - Es muss definiert sein, ob bei einem Ausdruck auch die Änderung und dessen Genehmigung ersichtlich sein müssen.
- Vertreterregelung
- Berechtigungskonzept
- Passwort-Management
- Management von Identifikations-Hardware
- Archivierung
- Verschlüsselung von vertraulichen Daten (wenn erforderlich, risikobasiert festzulegen)
- Umgang mit Änderungen signierter Daten (siehe Kapitel 4.1.2)

Tab. 10: Beispiel für User Requirements (Auszug).

Nr.	Anforderung
5.2.5	Sobald der Unterzeichnende den Signaturprozess beginnt, wird er darüber informiert, welchen Bearbeitungsschritt er im Begriff ist, auszuführen und in welcher Rolle er dies tut.
5.2.6	Der Benutzer wird aufgefordert, seinen Benutzernamen und sein Passwort einzugeben.
5.2.6.2	Das System weist den Benutzer zurück, falls die Eingaben nicht mit dem in der betreffenden Zeile im Signaturblock angegebenen Namen übereinstimmen.
5.2.6.3	Das System weist Benutzer mit falschem Passwort zurück.
5.2.8.3	Die Signaturinformation beinhaltet: <ul style="list-style-type: none"> <li>• Signaturtyp</li> <li>• Originalunterschrift</li> <li>• Vertreter</li> <li>• Abteilung</li> <li>• Datum- und Zeitstempel im UTC-Format</li> </ul>
5.4.3.5	Falls das Dokument durch den oben beschriebenen Prozess elektronisch unterschrieben wurde, wird auf der ersten Seite ein Text erstellt, der darüber informiert, dass die Bestätigung durch eine elektronische Signatur erfolgt ist.
5.4.6	Nachdem die letzte Unterschrift eingesetzt wurde, wird die Signaturinformation in das Audit Trail eingetragen.
5.4.7	Sowohl das PDF-Dokument als auch die Bewilligungsinformationen werden nach der letzten Unterschrift eingefroren.

Die festgelegten User Requirements beeinflussen entsprechend die nachfolgenden Spezifikations- und Design-Schritte (z. B. Functional Specifications, System Design Specifications, Software Design Specifications). In diesem Rahmen wird auch spezielles Signaturequipment (z. B. Kartenleser) in Abhängigkeit von der Art der zu verwendenden Signatur (z. B. qualifizierte elektronische Signatur) definiert.

Soweit eine systembezogene Risikoanalyse erstellt wird, sollten darin die mit der elektronischen Signatur verbundenen Risiken auf Basis der genannten Dokumente adäquat betrachtet werden.

#### 4.1.2 Änderungen signierter Daten

Der Sinn einer Signatur ist in erster Linie, Daten zu fixieren und zu bestätigen. Das bedeutet, dass Änderungen nicht vorgesehen sind und nur in speziellen Ausnahmefällen durchgeführt werden dürfen. Ausnahmen können z. B. Eingabefehler sein (z. B. Zahlendreher), die bei der Signatur übersehen wurden.

Nachfolgend wird detaillierter auf Änderungsprozesse signierter Daten eingegangen, die ggf. zu weiteren Anforderungen führen können. Hierbei sind folgende Aspekte zu berücksichtigen:

##### Freigabestatus der Daten

Die Änderungsprozesse sind abhängig vom Freigabestatus der Daten (z. B. „im Entwurf“, „geprüft“, „freigegeben“) zu definieren. Einmal per Signatur freigegebene Daten sollten nicht mehr ohne zusätzliche Signatur mit gleicher Befugnis geändert werden können.

##### Kritikalität der Daten

Im Sinne des „Risk-Based Approach“ sollte ein System so flexibel sein, dass in Abhängigkeit von der Kritikalität der Daten (z. B. Herstellbericht vs. Training-Handouts) unterschiedliche Änderungsprozesse etabliert und unterstützt werden.

##### Kritikalität des Fehlers

Stellt man z. B. Rechtschreibfehler oder nicht den Inhalt verfälschende Fehler (z. B. Korrektur von Seitennumerierungen) fest, so kann man unter Umständen diese zunächst belassen und erst in einer späteren Version mitkorrigieren. Handelt es sich um kritische Fehler, sollte eine zeitnahe Korrektur erfolgen.

##### Verknüpfung zwischen Daten und Signatur

Ausgehend von der gleichen Vorgehensweise, wie dies GxP-gerecht auf Papier erfolgen würde, muss bei Verwendung computerisierter Systeme spezifiziert sein, welche Daten mit welcher Signatur verknüpft sind.

Die unautorisierte Änderung von verknüpften Daten (Signatur und Electronic Record) darf außerhalb der Applikation und des zugehörigen Änderungsverfahrens nicht möglich sein. Für autorisierte Änderungen außerhalb der Applikation siehe Kapitel 4.3.4.

#### 4.2 Entwickler- und Abnahmetests

Die Erfüllung der signaturbezogenen Anforderungen aus User Requirements, Spezifikation und Design in Verbindung mit einer eventuell vorhandenen Risikoanalyse ist in Abhängigkeit von der Lieferantenbewertung im Rahmen der Entwickler- bzw. Abnahmetests zu überprüfen (siehe auch Tab. 11).

Tab. 11: Beispiel für Abnahmetests (Auszug).

Testfall-Nr.	Thema des Testfalles	Ziel	Testfall
19.15	Drei Signaturen – Negativtest nicht-korrekter User1	Ein nicht als der vorgesehene Benutzer identifizierter User darf nicht die Aktivität einfordern oder das Dokument unterschreiben.	[PBF00525]
19.21	Drei Signaturen – Sign1	Nach der vorherigen Ablehnung durch den dritten Unterschreibenden wird die erste Unterschrift dem Dokument korrekt hinzugefügt.	[PBF01034]
19.28	Drei Signaturen – Abschlusstest	Der Status des Dokumentes ist bestätigt. Attribute und Inhalte können nicht verändert werden.	[PBF00536]
19.32	Test Audit Trail – Bewilligung	Der Bewilligungsschritt eines Dokumentes wird in dem Audit Trail-Datenbestand richtig aufgezeichnet.	[PBF00662]

Fortsetzung Tabelle 1

Testfall-Nr.	Thema des Testfalles	Ziel	Testfall
19.33	Kopieren und Einfügen von Signatur-eintragungen	Negativtest: Elektronische Signaturen können nicht kopiert und in ein Entwurfsdokument im Forum eingefügt werden.	[PBF00500]
19.34	Löschen oder Modifizieren von elektronischen Signaturen	Negativtest: Elektronische Signatur-einträge können weder gelöscht noch verändert werden.	[PBF00501]

### 4.3 Systembetrieb

Mit Aufnahme des produktiven Betriebes muss zunächst im Sinne allgemein gültiger Anforderungen sichergestellt sein, dass ein System die ihm zugewiesenen Aufgaben auch nach Systemeinführung weiterhin ordnungsgemäß wahrnimmt. Nachstehend wird nur auf speziell zu berücksichtigende Aspekte, die mit dem Einsatz elektronischer Signaturen verbunden sind, eingegangen.

#### 4.3.1 Beschreibung fachlicher Abläufe

Die im Umfeld des Systems vorhandenen GxP-relevanten fachlichen Abläufe/Prozesse sind – soweit notwendig – unter Einbezug der Signaturfunktionen des Systems zu regeln.

#### 4.3.2 Schulung

Die Schulungen der Nutzer des Systems – aber auch der Administratoren – sind zu regeln und zu dokumentieren. Mindestens soll dabei auf folgende Punkte eingegangen werden:

- Äquivalenz der elektronischen Signatur zur handschriftlichen Unterschrift (bezogen auf 21 CFR Part 11 ist sicherzustellen, dass die Bestätigung gemäß Kapitel 3.1.1 eingeholt wird)
- Sorgfalt im Umgang mit der elektronischen Signatur analog der papiergestützten Unterschrift (z. B. Prüfung vor Unterschrift)
- Technische/organisatorische Fragen zur Einrichtung von Unterschriftsberechtigungen
- Technische/organisatorische Fragen zur Unterschriftsleistung im jeweiligen System
- Besondere Risiken der elektronischen Unterschrift im Vergleich zur handschriftlichen Unterschrift (z. B. Weitergabe/ Diebstahl des Zertifikates und des Passwortes)

#### 4.3.3 Berechtigungskonzept

Entscheidend für den Einsatz der elektronischen Signatur, gerade in Bezug auf die Sicherheit, ist das Berechtigungskonzept.

Es beinhaltet die Aspekte Authentisierung/Authentifizierung, Autorisierung und die Verwaltung der Berechtigungen.

Ziel ist die Sicherstellung, dass nur qualifizierte und autorisierte Personen Zugriff auf ein validiertes computerisiertes System bzw. auf kritische Systemfunktionalitäten erhalten. Dies bedeutet, dass alle Nutzer entsprechend geschult sein müssen; es sei denn, es geht um einen reinen Lesezugriff, für den keine besonderen Kenntnisse notwendig sind.

Bereits in den User Requirements sollte das Berechtigungskonzept behandelt werden (siehe Kapitel 4.1).

##### 4.3.3.1 Authentisierung / Authentifizierung

Für die Authentisierung stehen verschiedene Methoden zur Verfügung:

- Eingabe einer nur dem Nutzer bekannten Information (Passwort, PIN)
- Nutzung einer nur dem Nutzer zugänglichen Identifikations-Hardware (Karte, Schlüssel)
- Überprüfung biometrischer Merkmale

Um die Risiken einer vorgetäuschten Authentisierung zu minimieren, können Kombinationen aus zwei Komponenten genutzt werden (z. B. Karte plus Eingabe eines Passwortes). Die Nutzung biometrischer Informationen hat die größte inhärente Sicherheit, da eine Weitergabe der Informationen ausgeschlossen ist. Voraussetzung ist hierbei ein technisches System, welches eine eindeutige und komplikationsarme Erfassung der biometrischen Daten gewährleistet.

Die Authentifizierung erfolgt, indem die eingegebenen Daten vom System überprüft werden.

Die organisatorischen Maßnahmen im Zusammenhang mit der Authentifizierung sind abhängig von dem gewählten Authentifizierungsverfahren. Bei der am häufigsten verbreiteten Version der Nutzung eines Passwortes sind Maßnahmen zur Sicherstellung der Eindeutigkeit der Authentifizierung zu treffen. Da es vorkommen könnte, dass das gleiche Passwort von verschiedenen Personen genutzt wird, werden Anmeldekenndaten bestehend aus Nutzer-ID und Passwort verwendet.

Wegen der Notwendigkeit der Geheimhaltung des Passwortes ist die Eindeutigkeit der Kombination Nutzer-ID und Passwort dadurch zu gewährleisten, dass die Eindeutigkeit der bekannten Nutzer-ID sichergestellt wird. Des Weiteren muss sichergestellt werden, dass einmal vergebene Nutzer-IDs auch nach Ausscheiden von Mitarbeitern nicht ein zweites Mal zugewiesen werden. Dies ist organisatorisch zu regeln und in Arbeitsanweisungen festzuhalten.

Beispiele zur Sicherstellung der Eindeutigkeit der Nutzer-ID:

- Personalnummer ggf. in Kombination mit einer Standortkennung als ID
- Verwendung des Namens als ID, sofern bei Namensgleichheit Unterscheidungsmerkmale ergänzt werden (z. B. „Peter Müller\_1“)

Empfehlenswert ist eine Abstimmung mit der Personalabteilung, weil diese normalerweise für die Vergabe der Personalnummern zuständig ist.

#### **Passwort-Management**

Um die Sicherheit der korrekten Authentifizierung durch eine Verwendung von Passwörtern nicht zu gefährden, sollten eine regelmäßige Prüfung von technischen Passwort-Policies sowie regelmäßige Nachschulungen auf Basis der in den Unternehmen vorhandenen Regelungen zur Struktur und Gültigkeitsdauer von Passwörtern durchgeführt werden.

Die Regeln zur Erzeugung von persönlichen Codes sollten gemäß der APV-Richtlinie „Computergestützte Systeme“, basierend auf Annex 11 des EU-GMP-Leitfadens, folgende Angaben enthalten:

- Länge
- Verwendung von Sonderzeichen und Zeichenkombinationen
- - Gültigkeitsdauer
- Historie
- Verbotliste
- Regelung des Verhaltens, wenn der persönliche Code nicht mehr verfügbar bzw. nicht mehr geheim ist

Sind solche Regelungen unternehmensweit nicht vorhanden, sollten systemspezifische Regelungen geschaffen werden.

Zur Sicherstellung einer zeitlich begrenzten Gültigkeit von Passwörtern ist empfehlenswert, eine regelmäßige Änderung der Passwörter durch technische Maßnahmen per System zu erzwingen. Ist das nicht möglich, sollten die Nutzer per Anweisung verpflichtet werden, dies manuell zu tun.

Signaturversuche von nicht-ermächtigten Personen sollten erfasst werden. Dabei ist festzuhalten, zu welchem Zeitpunkt und an welchem System der misslungene Versuch erfolgte. Die so anfallenden Daten sollten regelmäßig im Rahmen der periodischen Überprüfungen analysiert und Folgemaßnahmen ergriffen werden.

Zu überprüfen ist darüber hinaus auch die verschlüsselte Übermittlung von Log-in-Daten. Dies ist um so wichtiger, wenn die technische Infrastruktur den Passwort-Abgleich aller vom Anwender im Unternehmen benutzten Systeme leistet (Single Sign-On). Es sollte dann gewährleistet sein, dass keines der Systeme das Passwort unverschlüsselt übermittelt, sodass ein Einbruchversuch mit einem Sniffer-Programm aussichtslos ist.

#### **Management von Identifikations-Hardware**

Auch bei der Nutzung von Identifikations-Hardware ist eine entsprechende Verwaltung notwendig. Gemäß der APV-Richtlinie "Computergestützte Systeme", basierend auf Annex 11 zum EU-GMP-Leitfaden, sind folgende Regelungen zu treffen:

- Vergabe- und Einzugsverfahren
- Ersatz bei Beschädigung oder Verlust sowie Folgemaßnahmen
- Führen einer Verteilerliste

#### **4.3.3.2 Autorisierung/Verwaltung der Berechtigungen**

Die Autorisierung setzt eine erfolgreiche Authentifizierung voraus und befasst sich mit der Zuweisung von Rechten.

Bei komplexeren Systemen sollte ein Rollenkonzept erstellt werden, bei dem bestimmte Rechte mit einer generischen Rolle verknüpft sind (z. B. Leser, Autor, Prüfer, Administrator). Im Regelfall ist der Systemeigner dafür zuständig, diese generischen Rollen den entsprechenden Personen zuzuweisen. Eine Schulung in angemessenem Umfang und auf sinnvolle Art und Weise (z. B. Lesen einer Kurzanleitung, Gruppenschulungen, ausführliche persönliche Einweisung usw.) sollte – neben dem Ausfüllen der Unterschriftenliste (s. o.) – Voraussetzung dafür sein.

#### **Entzug von Rechten**

Fast noch wichtiger und oft vernachlässigt ist eine Systematik zur regelmäßigen Aktualitätsprüfung (periodischer Review gemäß der Anforderung von 21 CFR Part 11.300 (b)) und zu dem daraus resultierenden Entzug von Rechten, speziell zur Leistung von elektronischen Signaturen. Dies gilt immer dann, wenn Mitarbeiter ihren Funktionsbereich wechseln oder das Unternehmen verlassen, aber auch bezogen auf Dummy-Accounts, die beispielsweise für bestimmte Validierungsaktivitäten eingerichtet wurden. Hier gibt es verschiedene Möglichkeiten, die kombiniert werden können:

- Automatisches Deaktivieren der Nutzer-ID, wenn der Nutzer sich über einen definierten Zeitraum hinweg nicht am System angemeldet hat
- Checklisten, die bei Personalbewegungen die Überprüfung der vorhandenen Zugriffsrechte auf IT-Systemen berücksichtigen
- Regelmäßige Überprüfung der Zugriffslisten

Sowohl bei der Zuweisung als auch beim Entzug von Rechten ist besonderes Augenmerk auf spezielle Berechtigungen zu legen. Angesprochen sind damit Benutzergruppen, die umfassende Rechte im System haben (Administratoren), aber auch Telearbeitsplätze oder externe Zugriffe, wie z. B. bei Fernwartungen. Bei Letzteren ist auf jeden Fall zu prüfen, ob und welche zusätzlichen Sicherheitsmaßnahmen zu treffen sind.

#### 4.3.4 Änderungskontrolle (Change Control)

##### Funktionale Änderungen

Bei funktionalen Änderungen an einem bestehenden System ist dafür zu sorgen, dass die Integrität bestehender und zukünftiger Signaturen erhalten bleibt und dass die zugehörigen Berechtigungen unter Kontrolle bleiben.

##### Änderungen an Daten zur Behebung von Störungen

Für notwendige Änderungen an fehlerhaften Daten einer GxP-relevanten Applikation, die infolge des Auftretens einer Störung generiert wurden, sind besondere Regelungen zu definieren.

Derartige Änderungen dürfen nur im (dokumentierten) Einverständnis mit dem Dateneigentümer erfolgen und sind nach einem definierten Änderungsverfahren abzuwickeln. Dieses ist im allgemeinen in einem standardisierten Verfahren zur Fehlerbehandlung festgelegt (unabhängig von der elektronischen Signatur). Dabei muss umfassend geprüft werden, wohin die signierten Daten vor der Änderung verteilt wurden. Davon ausgehend sind entsprechende Maßnahmen zu treffen (zumindest Information an die Empfänger und Übermittlung der korrigierten Version). Sind freigaberelevante Daten betroffen, so sind die entsprechenden Stellen zu informieren.

#### 4.3.5 Störungen

Im Betrieb eines Systems kann es aus unterschiedlichen Gründen zu technischen Störungen kommen.

Es ist zu definieren, an welche Stelle eine erkannte oder vermutete Störung zu melden ist, wie der weitere Ablauf der Störungsanalyse und ggf. -beseitigung aussieht und wie hierbei etwaige Einflüsse auf die Prozess-/Produktqualität oder Patientensicherheit ermittelt und berücksichtigt werden.

Sollte in Folge einer Störung eine Verletzung der Integrität geleisteter Unterschriften nicht auszuschließen sein, so ist dies ebenfalls als eine Beeinträchtigung der Prozess-/Produktqualität anzusehen.

#### 4.3.6 Abweichungen

Eine Abweichung ist die zeitlich begrenzte Verletzung bzw. Nichtbefolgung von in gültigen Dokumenten festgelegten Vorgaben. Die für das System gültige Abweichungsprozedur ist zu definieren. Im Regelfall sind keine spezifischen Aspekte hinsichtlich elektronischer Signaturen zu beachten.

#### 4.3.7 Datensicherung und Wiederherstellung

Datensicherung ist die Gesamtheit aller organisatorischen und technischen Vorsorgemaßnahmen gegen Verlust und/oder Verfälschung von Daten aufgrund von Katastrophen, technischen Ursachen, menschlichem Versagen oder mutwilligen Eingriffen.

Hierzu sind entsprechende Regelungen zu treffen. Diese sollten u. a. auch sicherstellen, dass im Falle von Integritätsverlusten elektronische Signaturen „wieder hergestellt“ werden können.

#### 4.3.8 Regelmäßige Systemüberwachung (Monitoring)

Ein geregeltes Monitoring hilft sicherzustellen, dass ein System während des gesamten Life Cycles ordnungsgemäß in Bezug auf die definierten Anforderungen und Spezifikationen arbeitet.

Diese Aktivitäten werden regelmäßig während des normalen Betriebes nach definierten Plänen durchgeführt. Sie sollen die Gegenstände des Monitorings (z. B. Leistung/Stabilität einer Komponente, Sicherheitsalarme), die Monitoring-Methode, vorgegebene Grenzwerte, Maßnahmen bei Überschreiten der Grenzen, die Häufigkeit des Monitorings und die entsprechende Durchführungsdokumentation beschreiben.

Das Monitoring leistet einen wesentlichen Beitrag zur Sicherstellung der Integrität der elektronischen Signaturen.

#### 4.3.9 Archivierung

Archivierung ist die Gesamtheit aller organisatorischen und technischen Vorsorgemaßnahmen mit dem Ziel, dass Daten inklusive der evtl. zugehörigen elektronischen Signaturen bis zum Ende der gesetzlich bzw. unternehmensintern festgelegten Archivierungsfrist verfügbar sind. Hinsichtlich elektronischer Signaturen bedeutet „Verfügbarkeit“ auch die Möglichkeit der Integritätsprüfung einer Unterschrift.

Die Thematik der Archivierung sollte bereits bei der Erstellung der User Requirements beachtet werden.

#### 4.3.10 Sicherheit und Notfallkonzept

Auch in Bezug auf die Integrität elektronischer Signaturen sind Regelungen zu treffen zur Sicherung von Systemen gegen:

- Informationsabfluss
- Manipulation
- Zerstörung
- Ausfall durch Nachlässigkeit
- Sabotage
- Defekte
- Unglücksfälle

Zusätzlich ist für den Notfall (definiert als länger dauernder Systemausfall) ein adäquates Konzept zu erstellen. Mit Blick auf elektronische Signaturen sollte dies auch eine Aussage beinhalten, ob und wie während der Ausfallzeit alternativ ggf. handschriftlich zu unterschreiben ist.

#### 4.3.11 Periodische Überprüfungen

Im Rahmen periodischer Überprüfungen wird der Validierungsstand eines Systems bewertet.

Hinsichtlich der elektronischen Signatur wird empfohlen, in diesem Zusammenhang die Aktualität der entsprechenden Unterschriftenberechtigungen zu prüfen.

#### 4.4 Außerbetriebnahme

Soll ein System außer Betrieb genommen werden, z. B. weil aufgrund der technischen Weiterentwicklung die bestehende Technologie zukünftig nicht mehr verfügbar sein wird, sind hinsichtlich signierter Daten u. a. folgende Varianten denkbar:

- Valide Migration auf ein Nachfolgesystem
- Valide Migration auf ein Hilfesystem (z. B. nur für Recherche- und Berichtszwecke)
- Ausdrucken und „notariell beglaubigen“
- Nachsignieren und Zertifikat erneuern

Dabei sind folgende Aspekte zu beachten:

- Einhaltung der gesetzlichen Aufbewahrungsfristen für Daten und Dokumente
- Dauer der Archivierung vs. Gültigkeitsdauer von elektronischen Signaturen
- Ggf. Regelung zur Schlüsselverwaltung (z. B. falls Zertifikate vor Ablauf der Archivierungsdauer ungültig werden)

### 5 Erläuterungen zur Public-Key-Infrastruktur (PKI)

Mittels der **asymmetrischen Verschlüsselung** können Nachrichten im Internet digital signiert und verschlüsselt werden. Allerdings wird hierzu der „**öffentliche Schlüssel**“ (**Public-Key**) des Absenders benötigt.

Damit sichergestellt ist, dass es sich tatsächlich um den öffentlichen Schlüssel des Absenders handelt und nicht um die Fälschung eines Betrügers, wird eine **vertrauenswürdige Stelle (Trust Center)** benötigt. Diese arbeitet als **Certification Authority (CA)** und stellt hierzu **Zertifikate** („Echtheitsbescheinigungen“) von öffentlichen Schlüsseln aus.

Die Verwaltung der Zertifikate durch eine CA wird in einer organisatorisch-technischen Umgebung, einer **Public-Key-Infrastruktur (PKI)**, durchgeführt. Sie besteht aus Technologie, Standards und definierten Sicherheitsanforderungen (Policy).

Die Policy definiert u. a. Haftung, Gewährleistung, Organisation, Standards, einzusetzende Technologie und deren Handhabung.

Eine PKI stellt Dienstleistungen wie Schlüssel-Management (Schlüsselerstellung, Aktualisierung, Wiedergewinnung, ...), Zertifikat-Management (Erzeugung, Bereitstellung, Erneuerung, Sperrung, ...) oder Zeitstempeldienste zur Verfügung. Zu einer PKI gehören folgende Komponenten:

- Die Zertifizierungsstelle (**Certification Authority – CA**) erstellt die digitalen Zertifikate für den Nutzer und verwaltet sie.
- Die Registrierungsstelle (**Registration Authority – RA**) verifiziert die Identität und Angaben des Antragstellers. Sie organisiert die Zertifikatsausgabe im Namen der CA.
- Der **Verzeichnisdienst** stellt eine öffentliche Datenbank zur Verfügung, in der Zertifikate geführt werden. Gesperrte Zertifikate werden über eine Sperrliste (**Certificate Revocation List – CRL**) gekennzeichnet.
- Eine Alternative zur CRL ist das „Online Certificate Status Protocol“ (OCSP), mit dem der Status eines Zertifikates online überprüft werden kann.
- Der **Zeitstempeldienst** bestätigt die Vorlage von digitalen Daten zu einem bestimmten Zeitpunkt – dies ist von besonderer Bedeutung bei Verträgen und Urkunden.

Jede Organisation oder jedes Unternehmen, das den internen und/oder externen Datenaustausch sicher gestalten möchte und sich entscheidet, mit Zertifikaten zu arbeiten, kann seine eigene PKI aufbauen und einsetzen. Dabei kann die

Firma/Organisation den organisatorischen und technischen Betrieb der PKI selbst übernehmen oder Dienste eines externen Dienstleisters (**Certification Service Provider – CSP**) nutzen.

Die gegenseitige Anerkennung unterschiedlicher PKIs kann über eine **Bridge-CA** vereinfacht werden.

## 6 Glossar

<b>Audit Trail</b>	Systemseitiger Protokollmechanismus, der es ermöglicht, jede Dateneingabe bzw. Weiterverarbeitung von Daten durch das System auf die Originaldaten zurückzuführen (APV-Interpretation Annex 11).
<b>Authentifizierung</b>	Identitätsprüfung der berechtigten Nutzer bei der Anmeldung in ein Computersystem.
<b>Authentisierung</b>	Nachweis der eigenen Identität bei der Anmeldung in ein Computersystem.
<b>Autorisierung</b>	Zuweisung von Rechten.
<b>Biometrische Methode</b>	Methode zum Nachweis der Identität einer Person basierend auf physischen Eigenschaften oder wiederholbaren Handlungen, die die Person eindeutig kennzeichnen und messbar sind.
<b>digital signature</b>	Definition gemäß 21 CFR Part 11: electronic signature basierend auf kryptografischen Methoden der Urheberauthentisierung. Zur Verschlüsselung werden jeweils ein Regel- und ein Parametersatz verwendet, um die Urheberidentität und die Datenintegrität zu verifizieren.
<b>electronic signature</b>	Definition gemäß 21 CFR Part 11: mittels Computertechnik verarbeitete Symbol oder Symbolserien, die von einer Person ausgeführt, angewendet oder autorisiert wurde, um als rechtsgültiges verbindliches Äquivalent zur handschriftlichen Unterschrift zu gelten.
<b>Elektronische Signatur (einfache)</b>	Laut Signaturgesetz (SigG) Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen.
<b>Elektronische Form</b>	Laut § 126b BGB entspricht die elektronische Form einer Umsetzung der Schriftform in elektronischen Medien. Hierbei muss das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz unterzeichnet werden.
<b>Fortgeschrittene elektronische Signatur</b>	Laut Signaturgesetz (SigG) elektronische Signaturen, die a) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind, b) die Identifizierung des Signaturschlüssel-Inhabers ermöglichen, c) mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und d) mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann, ...
<b>Geschlossenes System</b>	Definition gemäß 21 CFR Part 11: Umgebung, in der der Systemzugang durch diejenigen Personen kontrolliert wird, die für den Inhalt der elektronischen Dokumente verantwortlich sind.
<b>Hybrid-System</b>	System, in dem elektronische und Papierdokumente eingesetzt werden. In den meisten Fällen werden Aufzeichnungen elektronisch erzeugt, und zum Zwecke der Unterzeichnung werden die Dokumente ausgedruckt und auf Papier unterschrieben. Im Sinne des 21 CFR Part 11 liegen in diesem Fall zwar ggf. electronic records vor (die Daten, die zum Ausdruck des Papiers geführt haben), aber keine electronic signature, da die Unterschrift auf Papier erfolgt.
<b>Offenes System</b>	Definition gemäß 21 CFR Part 11: Umgebung, in der der Systemzugang nicht durch diejenigen Personen kontrolliert wird, die für den Inhalt der elektronischen Dokumente verantwortlich sind.
<b>Qualifizierte elektronische Signatur</b>	Laut Signaturgesetz (SigG) fortgeschrittene elektronische Signaturen die a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und b) mit einer sicheren Signaturerstellungseinheit erzeugt werden.
<b>Schriftform</b>	Laut § 126b BGB entspricht eine Erklärung der Schriftform, wenn sie vom Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigtem Handzeichen unterzeichnet wurde.
<b>Single Sign-On</b>	Mit einmaliger Anmeldung/Authentisierung Zugriff auf sämtliche Systeme, für die der Anwender eine Berechtigung hat.
<b>Sniffer-Programm</b>	Ein Sniffer-Programm ist ein Werkzeug der LAN-Analyse. Man kann damit den Datenverkehr eines Netzwerks empfangen, aufzeichnen, darstellen und ggf. auswerten. Ein solches Programm kann aber auch zur Datenspionage eingesetzt werden.
<b>Textform</b>	Laut § 126b BGB entspricht eine Erklärung der Textform, wenn sie in einer Urkunde oder auf andere zur dauerhaften Wiedergabe in Schriftzeichen geeigneten Weise abgegeben, die Person des Erklärenden genannt und der Abschluss der Erklärung durch Nachbildung der Namensunterschrift oder anders erkennbar gemacht werden.  Bei der Textform ist also keine Unterschrift erforderlich.

## 7 Abkürzungen

AMG	Arzneimittelgesetz
AMG-EV	AMG-Einreichungsverordnung
AMVV	Arzneimittelverschreibungsverordnung
AMWHV	Arzneimittel- und Wirkstoffherstellungsverordnung
APV	Arbeitsgemeinschaft für Pharmazeutische Verfahrenstechnik e.V.
BGB	Bürgerliches Gesetzbuch
CFR	Code of Federal Regulations
cGMP	Current Good Manufacturing Practices
ChemVwV-GLP	Allgemeine Verwaltungsvorschrift zum Verfahren der behördlichen Überwachung der Einhaltung der Grundsätze der Guten Laborpraxis
DHR	Device History Record
DMS	Dokumenten-Management-System
DV	Datenverarbeitung
ES	Elektronische Signatur
FDA	Food and Drug Administration
GAMP	Good Automated Manufacturing Practice
GCP	Good Clinical Practice
GLP	Good Laboratory Practice, Gute Laborpraxis
GMP	Good Manufacturing Practice
GxP	Zusammenfassung der Good Practices: Zu den GxP gehören unter anderem: <ul style="list-style-type: none"> <li>• Good Manufacturing Practice (GMP)</li> <li>• Good Distribution Practice (GDP)</li> <li>• Good Clinical Practice (GCP)</li> <li>• Good Laboratory Practice (GLP)</li> <li>• Good Automated Manufacturing Practice (GAMP)</li> </ul>
ICH	International Conference on Harmonisation
ID	Identifikationskennung
IT	Informationstechnologie
IVD-Direktive	In-vitro Diagnostic Medical Devices Directive
MPG	Medizinproduktegesetz
OECD	Organisation for Economic Co-operation and Development, Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
PDF	Portable Document Format
PIN	Persönliche Identifikationsnummer (i. d. R. nur Ziffern)
PKI	Public Key Infrastructure
PW	Passwort
QM	Qualitätsmanagement
QS	Qualitätssicherung
SigG	Signaturgesetz
SOP	Standard Operating Procedure, Standardarbeitsanweisung
URS	User Requirement Specification
UTC	Universal Time Coordinated, koordinierte Weltzeit

## 8 Literaturhinweise

- K. Clevermann, R. Hössel, C. Hornberger, E. Klappauf, T. Linz, M. Schulz, „Einsatz von elektronischen Signaturen im pharmazeutischen Umfeld“, Pharm. Ind. **68**, 552 (2006)
- GAMP-Good Practice Guide: A Risk-Based Approach to Compliant Electronic Records and Signatures
- M. Fischlin, A. Giessler, R. Nitschke, H. Rittner (Projektgruppe E-Government im Bundesamt für Sicherheit in der Informationstechnik) „Verschlüsselung und Signatur – Grundlagen und Anwendungsaspekte“, <http://www.e-government-handbuch.de> (2005)
- D. Gassen, „Digitale Signaturen in der Praxis“, Verlag Dr. Otto Schmitt, Köln (2003)
- C. J. Langenbach, O. Ulrich (Hrsg.), „Elektronische Signaturen“, Springer-Verlag, Berlin–Heidelberg–New York (2002)

## 9 Nützliche Links und Adressen

### Internet-Links zum Thema Zertifizierung und Signaturen

- Teletrust: [www.teletrust.de](http://www.teletrust.de)
- Verwaltungs-PKI: [www.bsi.de/fachthem/verwpki/index.htm](http://www.bsi.de/fachthem/verwpki/index.htm)
- Spezifikationen: [www.isis-mtt.org](http://www.isis-mtt.org)
- Signaturländnis: [www.signaturlaendnis.de](http://www.signaturlaendnis.de)
- BMWI: [www.zukunft-ebusiness.de/E-Business/Navigation/Recht/deutschland.html](http://www.zukunft-ebusiness.de/E-Business/Navigation/Recht/deutschland.html)
- Bundesnetzagentur: [www.bundesnetzagentur.de](http://www.bundesnetzagentur.de)
- Verein zur Förderung elektronischer Signatur: [www.siglab.de](http://www.siglab.de)

### Auswahl einiger Zertifizierungsstellen

- Telesec/T-Systems, 1998, Z0001
- Deutsche Post SignTrust, 2000, Z0002
- Bundesnotarkammer, 2002, Z0003
- DATEV eG, 2001, Z0004 (Steuerberater und Rechtsanwaltskammer in 2001 und 2002)
- Authentidate, 2001, Z0015 (Zeitstempel)
- TC Trustcenter, 2001, Z0016
- D-Trust, 2002, Z0017

## 10 Anhang

Auswahl relevanter Richtlinien und Gesetzestexte (Auszüge)

## 10 Anhang

### Auswahl relevanter Richtlinien und Gesetzestexte (Auszüge)

Tabelle 1: Arzneimittel- und Wirkstoffherstellungsverordnung (Forderung nach Unterschrift)	II
Tabelle 2: Arzneimittel- und Wirkstoffherstellungsverordnung (keine explizite Forderung nach Unterschrift)	III
Tabelle 3: 21 CFR Part 210/211	V
Tabelle 4: Chemikaliengesetz	VI
Tabelle 5: Richtlinie 2004/10/EG	VIII
Tabelle 6: OECD GLP-Konsensdokumente	IX
Tabelle 7: Neufassung Allgemeine Verwaltungsvorschrift (ChemVwV-GLP)	X
Tabelle 8: Arzneimittelgesetz (GCP)	XI
Tabelle 9: Verordnung über die Anwendung der Guten Klinischen Praxis	XI

Tab. 1: Arzneimittel- und Wirkstoffherstellungsverordnung (AMWHV) – relevante Auszüge hinsichtlich Forderung nach Unterschrift.

§§ AMWHV (§§ der alten PharmBetrV)	Absatz aus AMWHV
<b>Abschnitt 3: Arzneimittel, Blutprodukte, Produkte menschlicher Herkunft</b>	
§ 13 Herstellung  (vgl. PharmBetrV § 5 Herstellung)	(7) Die Herstellung jeder Charge ist gemäß der Herstellungsanweisung nach Absatz 1 durchzuführen und vollständig zu protokollieren (Herstellungsprotokoll). Alle Abweichungen im Prozess und von der Festlegung der Spezifikation sind zu dokumentieren und gründlich zu untersuchen. Soweit das Produkt nicht in Chargen hergestellt wird, gilt Satz 1 entsprechend.  (8) Im Herstellungsprotokoll ist von der Leitung der Herstellung <b>mit Datum und Unterschrift zu bestätigen</b> , dass die Charge entsprechend der Herstellungsanweisung hergestellt wurde.
§ 14 Prüfung  (vgl. PharmBetrV § 6 Prüfung)	(4) Die Prüfung ist gemäß der Prüfanweisung nach Absatz 1 durchzuführen und vollständig zu protokollieren (Prüfprotokoll). Alle Abweichungen im Prozess und von der Festlegung in der Spezifikation sind zu dokumentieren und gründlich zu untersuchen. Die Leitung der Qualitätskontrolle hat im Prüfprotokoll <b>mit Datum und Unterschrift zu bestätigen</b> , dass die Prüfung entsprechend der Prüfanweisung durchgeführt worden ist und das Produkt die erforderliche Qualität besitzt.  (6) Ausgangsstoffe, Zwischen- und Endprodukte, die den Anforderungen an die Qualität nicht genügen, sind als solche kenntlich zu machen und abzusondern. Über die weiteren Maßnahmen ist von dazu befugtem Personal zu entscheiden. Die Maßnahmen <b>sind zu dokumentieren</b> .
§ 16 Freigabe zum Inverkehrbringen  (vgl. PharmBetrV § 7 Freigabe)	(2) Die Freigabe darf nur erfolgen, wenn 1. das Herstellungsprotokoll und das Prüfprotokoll <b>ordnungsgemäß unterzeichnet</b> sind, 2. zusätzlich zu den analytischen Ergebnissen essentielle Informationen wie die Herstellungsbedingungen und die Ergebnisse der Inprozesskontrollen berücksichtigt wurden, 3. die Überprüfung der Herstellungs- und Prüfunterlagen die Übereinstimmung der Produkte mit ihren Spezifikationen, einschließlich der Endverpackung, bestätigt hat und 4. bei ...
§ 17 Inverkehrbringen und Einfuhr  (vgl. PharmBetrV § 13 Vertrieb und Einfuhr)	(2) Bei einem Verbringen aus einem Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum in den Geltungsbereich des Arzneimittelgesetzes kann von der Prüfung nach Absatz 1 abgesehen werden, wenn die Prüfung in dem Mitgliedstaat oder in dem anderen Vertragsstaat nach den dort geltenden Rechtsvorschriften durchgeführt und die von der sachkundigen Person <b>unterzeichneten Kontrollberichte</b> beigelegt wurden.
<b>Abschnitt 4: Wirkstoffe nicht-menschlicher Herkunft</b>	
§ 22 Herstellung  (vgl. PharmBetrV § 25 Produktion)	(7) Im Herstellungsprotokoll ist in Betrieben und Einrichtungen, die der Erlaubnispflicht nach § 13 des Arzneimittelgesetzes unterliegen, von der Leitung der Herstellung <b>mit Datum und Unterschrift zu bestätigen</b> , dass die Charge entsprechend der Herstellungsanweisung hergestellt wurde. In anderen Betrieben und Einrichtungen sind eine oder mehrere entsprechende Personen festzulegen, die für die Überprüfung der Protokolle auf Vollständigkeit und Richtigkeit verantwortlich sind.
§ 23 Prüfung  (vgl. PharmBetrV § 26 Laborkontrollen)	(5) In Betrieben und Einrichtungen, die einer Erlaubnis nach § 13 des Arzneimittelgesetzes bedürfen, hat die Leitung der Qualitätskontrolle im Prüfprotokoll <b>mit Datum und Unterschrift zu bestätigen</b> , dass die Prüfung entsprechend der Prüfanweisung durchgeführt worden ist und das Produkt die erforderliche Qualität besitzt. In anderen Betrieben und Einrichtungen sind entsprechende Verantwortlichkeiten festzulegen.  (7) Ausgangsstoffe, Zwischenprodukte und Wirkstoffe, die den Anforderungen an die Qualität nicht genügen, sind als solche kenntlich zu machen und abzusondern. Über die weiteren Maßnahmen ist von dazu befugtem Personal zu entscheiden. Die Maßnahmen sind zu dokumentieren.

§§ AMWHV (§§ der alten PharmBetrV)	Absatz aus AMWHV
§ 25 Freigabe zum Inverkehrbringen	(3) Die Freigabe nach Absatz 1 darf nur erfolgen, wenn das Herstellungsprotokoll und das Prüfprotokoll ordnungsgemäß unterzeichnet sind, zusätzlich zu den analytischen Ergebnissen essentielle Informationen wie die Herstellungsbedingungen und die Ergebnisse der Inprozesskontrollen berücksichtigt wurden und die Überprüfung der Herstellungs- und Prüfunterlagen die Übereinstimmung der Produkte mit ihren Spezifikationen bestätigt hat. (4) Bei Zwischenprodukten und Wirkstoffen, die ausschließlich umgefüllt, abgefüllt, abgepackt oder gekennzeichnet werden, darf die Freigabe nach Absatz 1 nur erfolgen, wenn <ol style="list-style-type: none"> <li>1. mindestens die Identität dieser Produkte festgestellt wurde und darüber ein <b>ordnungsgemäß unterzeichnetes Prüfprotokoll</b> vorliegt,</li> <li>2. über das Umfüllen, Abfüllen, Abpacken und Kennzeichnen ein <b>ordnungsgemäß unterzeichnetes Herstellungsprotokoll</b> vorliegt,</li> <li>3. ...</li> </ol>
§ 10 Allgemeine Dokumentation  (vgl. PharmBetrV § 15 Dokumentation)	Hier wird jedoch ausdrücklich auf die Verwendung elektronischer Medien eingegangen: (2) Werden die Aufzeichnungen mit elektronischen, photographischen oder anderen Datenverarbeitungssystemen gemacht, ist das System ausreichend zu validieren. Es muss mindestens sichergestellt sein, dass die Daten während der Dauer der Aufbewahrungsfrist verfügbar sind und innerhalb einer angemessenen Frist lesbar gemacht werden können. Die gespeicherten Daten müssen gegen Verlust und Beschädigung geschützt werden. <b>Wird ein System zur automatischen Datenverarbeitung oder -übertragung eingesetzt, so genügt statt der eigenhändigen Unterschrift der jeweils verantwortlichen Personen deren Namenswiedergabe, wenn in geeigneter Weise sichergestellt ist, dass nur befugte Personen die Bestätigung über die ordnungsgemäße Ausführung der jeweiligen Tätigkeiten vornehmen können.</b>

Tab. 2: Arzneimittel- und Wirkstoffherstellungsverordnung (AMWHV) – relevante Auszüge, nach denen jeweils nur schriftliche Vorgaben bzw. Dokumentation, aber ohne explizite Unterschrift, gefordert sind.

AMWHV	Absatz aus AMWHV
<b>Abschnitt 3: Arzneimittel, Blutprodukte, Produkte menschlicher Herkunft</b>	
§ 6 Hygienemaßnahmen	(1) Betriebsräume und ihre Ausrüstungen müssen regelmäßig gereinigt und, soweit erforderlich, desinfiziert oder sterilisiert werden. Es soll nach einem <b>schriftlichen Hygieneplan</b> verfahren werden, in dem insbesondere ... (2) Unbeschadet des Hygieneplans nach Absatz 1 müssen <b>schriftliche Hygieneprogramme</b> vorhanden sein, die den durchzuführenden Tätigkeiten angepasst sind.
§ 7 Lagerung und Transport	(5) Die Verfahren für die Lagerung und den Transport sind <b>schriftlich festzulegen</b> .
§ 11 Selbstinspektion und Lieferantenqualifizierung	(2) Die Qualifizierung von Lieferanten für Ausgangsstoffe und primäre und sekundäre Verpackungsmaterialien, die zur Arzneimittelherstellung eingesetzt werden, ist im Rahmen des QM-Systems des verarbeitenden Betriebes nach <b>schriftlich festgelegtem Verfahren</b> durchzuführen.
§ 12 Personal in leitender und verantwortlicher Stellung	(1) Der Verantwortungsbereich der sachkundigen Person ist nach Maßgabe von § 19 des Arzneimittelgesetzes <b>schriftlich festzulegen</b> . Die Aufgaben der Leitung der Herstellung und der Leitung der Qualitätskontrolle sind ebenfalls <b>schriftlich festzulegen</b> .
§ 13 Herstellung	(1) Die Herstellungsvorgänge sind mit Ausnahme der Freigabe unter Verantwortung der Leitung der Herstellung nach vorher erstellten <b>schriftlichen Anweisungen</b> und Verfahrensbeschreibungen (Herstellungsanweisung) durchzuführen.

AMWHV	Absatz aus AMWHV
§ 14 Prüfung	(1) Ausgangsstoffe und Endprodukte sowie erforderlichenfalls auch Zwischenprodukte sind unter Verantwortung der Leitung der Qualitätskontrolle nach vorher erstellten <b>schriftlichen Anweisungen</b> und Verfahrensbeschreibungen (Prüfanweisung) zu prüfen.
§ 16 Freigabe zum Inverkehrbringen	(1) Die Freigabe einer Charge zum Inverkehrbringen darf von der sachkundigen Person nach § 14 des Arzneimittelgesetzes, die mit dem Produkt und mit den für dessen Herstellung und Prüfung eingesetzten Verfahren vertraut ist, nur nach von ihr <b>vorher erstellten schriftlichen Anweisungen</b> und Verfahrensbeschreibungen nach Absatz 2 oder 3 Satz 2 vorgenommen werden.
§ 19 Beanstandungen und Rückruf	(1) Der oder die Stufenplanbeauftragte ist dafür verantwortlich, dass alle bekannt gewordenen Meldungen über Arzneimittelrisiken nach <b>schriftlich festgelegtem Verfahren</b> gesammelt sowie alle Beanstandungen systematisch aufgezeichnet werden.
§ 22 Herstellung	(1) Die Herstellungsvorgänge einschließlich der Inprozesskontrollen sind nach <b>vorher erstellten schriftlichen Anweisungen und Verfahrensbeschreibungen</b> (Herstellungsanweisung) und in Übereinstimmung mit der Guten Herstellungspraxis durchzuführen.
§ 23 Prüfung	(1) Ausgangsstoffe, Zwischenprodukte und Wirkstoffe sind nach <b>vorher erstellten schriftlichen Anweisungen und Verfahrensbeschreibungen</b> (Prüfanweisung) und in Übereinstimmung mit der Guten Herstellungspraxis zu prüfen.
§ 24 Kennzeichnung	(1) Die Kennzeichnung der Zwischenprodukte und Wirkstoffe ist nach <b>vorher erstellten schriftlichen Anweisungen</b> und Verfahrensbeschreibungen und in Übereinstimmung mit der Guten Herstellungspraxis durchzuführen.
§ 25 Freigabe zum Inverkehrbringen	(1) Die Freigabe zum Inverkehrbringen darf nur nach <b>vorher erstellten schriftlichen Anweisungen und Verfahrensbeschreibungen</b> nach Absatz 3 oder Absatz 4 Satz 1 von Personen vorgenommen werden, die mit den Produkten und mit den für deren Herstellung und Prüfung eingesetzten Verfahren vertraut sind. (2) ... die zur Freigabe berechtigten Personen sind schriftlich festzulegen.
§ 28 Beanstandungen und Rückruf	(1) Alle qualitätsbezogenen Beanstandungen sind in Betrieben und Einrichtungen, die Wirkstoffe im Geltungsbereich des Arzneimittelgesetzes herstellen oder in den Geltungsbereich des Gesetzes verbringen oder einführen, von der Qualitätssicherungseinheit <b>nach schriftlich festgelegtem Verfahren</b> zu dokumentieren, zu untersuchen und zu bewerten. (2) ... Die Voraussetzungen, unter denen ein Produktrückruf in Betracht zu ziehen ist, sowie das Rückrufverfahren selbst sind schriftlich festzulegen.
§ 30 Ergänzende Regelungen für Fütterungsarzneimittel	(5) Abweichend von § 16 kann in Fällen kurzfristiger Verhinderung anstelle der sachkundigen Person nach § 14 des Arzneimittelgesetzes eine beauftragte Person, die über ausreichende Ausbildung und Kenntnisse verfügt, Fütterungsarzneimittel vorläufig für das Inverkehrbringen freigeben. Diese vorläufige Freigabe ist nachträglich der sachkundigen Person, die auch in diesem Falle neben der beauftragten Person die Verantwortung für die Freigabe trägt, vorzulegen und von dieser <b>schriftlich zu bestätigen</b> .
§ 31 Ergänzende Regelungen für Blutspendeinrichtungen	(10) Abweichend von § 16 kann in Fällen kurzfristiger Verhinderung und wenn dies aus medizinischen Gründen dringend erforderlich ist, anstelle der sachkundigen Person nach § 14 des Arzneimittelgesetzes eine beauftragte Person, die über ausreichende Ausbildung und Kenntnisse verfügt, die Blutzubereitungen zur unmittelbaren Anwendung bei Menschen vorläufig für das Inverkehrbringen freigeben und den Eintrag nach § 17 Abs. 5 vornehmen. Diese vorläufige Freigabe und der vorläufige Eintrag nach § 17 Abs. 5 sind nachträglich der sachkundigen Person, die auch in diesem Falle neben der beauftragten Person die Verantwortung für die Freigabe trägt, vorzulegen und von dieser <b>schriftlich zu bestätigen</b> .

Tab. 3: 21 CFR Part 210/211.

§§	Absatz	
211.22	<b>Responsibilities of quality control unit</b> ... a quality control unit that shall have the responsibility and authority to <b>approve or reject</b> all components, drug product containers ...	Approval
211.84	<b>Testing and approval or rejection of components, drug product containers, and closures</b> ... (e) Any lot of components, drug product containers, or closures that meets the appropriate written specifications of identity, strength, quality, and purity and related tests under paragraph (d) of this section may be <b>approved and released</b> for use. Any lot of such material that does not meet such specifications shall be rejected ...	Approval
211.87	<b>Retesting of approved components, drug product containers, and closures</b> Components, drug product containers, and closures shall be retested or reexamined, as appropriate, for identity, strength, quality, and purity and <b>approved or rejected</b> by the quality control unit in accordance with § 211.84 as necessary.	Approval
211.100 (a)	<b>Written procedures; deviations</b> ... These written procedures, including any changes, shall be drafted, reviewed, and approved by the appropriate organizational units and reviewed and <b>approved</b> by the quality control unit ...	Approval
211.110	<b>Sampling and testing of in-process materials and drug products</b> (c) In-process materials shall be tested for identity, strength, quality, and purity as appropriate, and <b>approved or rejected</b> by the quality control unit, during the production process, e.g., at commencement or completion of significant phases or after storage for long periods.	Approval
211.115	<b>Reprocessing</b> (b) Reprocessing shall not be performed without the review and approval of the quality control unit.	Approval
211.122	<b>Materials examination and usage criteria</b> (b) Any labeling or packaging materials meeting appropriate written specifications may be <b>approved and released</b> for use. Any labeling or packaging materials that do not meet such specifications shall be rejected to prevent their use in operations for which they are unsuitable.	Approval
211.160	<b>General requirements for laboratory controls</b> (a) The establishment of any specifications, standards, sampling plans, test procedures, or other laboratory control mechanisms required by this subpart, including any change in such specifications, standards, sampling plans, test procedures, or other laboratory control mechanisms, shall be drafted by the appropriate organizational unit and reviewed and <b>approved</b> by the quality control unit.	Approval
211.182	<b>Equipment cleaning and use log</b> ... The persons performing and double-checking the cleaning and maintenance shall date and sign or initial the log indicating that the work was performed.	Approval

§§	Absatz	Gefordert
211.186 (a), (b) 8)	<p><b>Master production and control records</b></p> <p>(a) To assure uniformity from batch to batch, master production and control records for each drug product, including each batch size thereof, shall be prepared, dated, and signed (full signature, handwritten) by one person and independently checked, dated, and signed by a second person. ...</p> <p>(b)(8) A description of the drug product containers, closures, and packaging materials, including a specimen or copy of each label and all other labeling signed and dated by the person or persons responsible for approval of such labeling;</p>	Signature
211.188 (a)	<p><b>Batch production and control records</b></p> <p>Batch production and control records shall be prepared for each batch of drug product produced and shall include complete information relating to the production and control of each batch. These records shall include:</p> <p>(a) An accurate reproduction of the appropriate master production or control record, checked for accuracy, dated, and signed;</p>	Signature
211.188 (b)	<p><b>Batch production and control records</b></p> <p>b) Documentation that each significant step in the manufacture, processing, packing, or holding of the batch was accomplished, including:</p> <p>(1) Dates;</p> <p>(2) Identity of individual major equipment and lines used;</p> <p>(3) ...</p>	Identity of individual
211.192	<p><b>Production record review</b></p> <p>All drug product production and control records, including those for packaging and labeling, shall be reviewed and <b>approved</b> by the quality control unit to determine compliance with all established, approved written procedures before a batch is released or distributed ...</p>	Approval
211.194 (a), 7), 8)	<p><b>Laboratory records</b></p> <p>(7) The <b>initials or signature</b> of the person who performs each test and the date(s) the tests were performed.</p> <p>(8) The <b>initials or signature</b> of a second person showing that the original records have been reviewed for accuracy, completeness, and compliance with established standards.</p>	Initial or signature

Tab. 4: Chemikaliengesetz (ChemG) in der Fassung der Bekanntmachung vom 20. Juni 2002 (BGBl. I S. 2090); zuletzt geändert durch Artikel 2 § 3 Absatz 6 des Gesetzes vom 1. September 2005 (BGBl. I S. 2618)).

Abschnitte	Absatz aus dem ChemG, Anhang 1 zu § 19a Abs. 1, Grundsätze der Guten Laborpraxis	Gefordert
Abschnitt II, 1.2: Aufgaben des Prüfleiters	Der Prüfleiter hat den Prüfplan sowie etwaige Änderungen durch <b>datierte Unterschrift</b> zu genehmigen. ...	Unterschrift

Abschnitte	Absatz aus dem ChemG, Anhang 1 zu § 19a Abs. 1, Grundsätze der Guten Laborpraxis	Gefordert
	... den Abschlussbericht <b>datiert zu unterzeichnen</b> , um damit die Verantwortung für die Zuverlässigkeit der Daten zu übernehmen und anzugeben, inwieweit die Prüfung mit diesen Grundsätzen der Guten Laborpraxis übereinstimmt.	Unterschrift
Abschnitt II, 2.2: Aufgaben des Qualitätssicherungs- personals	Das Qualitätssicherungspersonal hat zumindest ... eine dem Abschlussbericht beizufügende Erklärung abzufassen und <b>zu unterzeichnen</b> , aus der Art und Zeitpunkt der Inspektionen, die inspizierten Phasen der Prüfung sowie die Zeitpunkte, an denen der Leitung und dem Prüfleiter sowie gegebenenfalls einem Örtlichen Versuchsleiter Inspektionsergebnisse berichtet wurden, hervorgehen. Weiterhin dient diese Erklärung als Bestätigung, dass der Abschlussbericht die Rohdaten widerspiegelt.	Unterzeichnen
Abschnitt II, 8.1: Prüfplan	Vor Beginn der Prüfung muss ein schriftlicher Prüfplan vorliegen. Der Prüfplan muss vom Prüfleiter durch <b>datierte Unterschrift</b> genehmigt werden. ... Prüfplanänderungen müssen begründet und durch <b>datierte Unterschrift</b> des Prüflleiters genehmigt werden und sind gemeinsam mit dem Prüfplan aufzubewahren.	Unterschrift
Abschnitt II, 8.3: Durchführung der Prüfung	Alle während der Prüfung erhobenen Daten sind durch die erhebende Person unmittelbar, unverzüglich, genau und leserlich <b>zu unterschreiben oder abzuzeichnen</b> .	Abzeichnen
	Jede Änderung in den Rohdaten ist so vorzunehmen, dass die ursprüngliche Aufzeichnung ersichtlich bleibt. Sie ist mit einer Begründung sowie <b>Datum und Unterschrift oder Kürzel</b> der die Änderung vornehmenden Person zu versehen.	Kürzel
	Daten, die als direkte Computereingabe entstehen, sind zur Zeit der Dateneingabe durch die dafür verantwortliche Person <b>zu kennzeichnen</b> . Computergestützte Systeme müssen so ausgelegt sein, dass jederzeit die Aufzeichnung eines vollständigen Audit Trails zur Verfügung steht, der sämtliche Datenänderungen anzeigt, ohne die Originaldaten unkenntlich zu machen. Alle Datenänderungen müssen mit der sie ändernden Person verknüpft werden können, z. B. durch die Verwendung der mit <b>Datum und Unterschrift versehenen (elektronischen) Unterschriften</b> .	Elektronische Unterschrift
Abschnitt II 9: Bericht über die Prüfergebnisse	Jeder Bericht eines an der Prüfung beteiligten Örtlichen Versuchsleiters oder beteiligten Spezialisten ist von diesem <b>datiert zu unterschreiben</b> .	Unterschrift
	Der Abschlussbericht muss vom Prüfleiter <b>datiert unterschrieben</b> werden, um die Übernahme der Verantwortung für die Zuverlässigkeit der Daten zu dokumentieren. Des weiteren ist anzugeben, inwieweit die Prüfung mit diesen Grundsätzen der Guten Laborpraxis übereinstimmt.	Unterschrift
	Korrekturen und Ergänzungen eines Abschlussberichtes sind in Form von Nachträgen vorzunehmen. In diesen Nachträgen sind die Gründe für die Korrekturen oder Ergänzungen deutlich darzulegen und vom Prüfleiter <b>datiert zu unterzeichnen</b> .	Unterschrift

Tab. 5: Richtlinie 2004/10/EG des Europäischen Parlamentes und des Rates vom 11. Februar 2004 zur Angleichung der Rechts- und Verwaltungsvorschriften für die Anwendung der Grundsätze der Guten Laborpraxis und zur Kontrolle ihrer Anwendung bei Versuchen mit chemischen Stoffen (kodifizierte Fassung).

Absatz	Absatz aus EG-Richtlinie	Gefordert
Aufgaben des Prüfleiters	Der Prüfleiter hat den Prüfplan sowie etwaige Änderungen durch <b>datierte Unterschrift</b> zu genehmigen; ...	Unterschrift
	Der Prüfleiter hat den Abschlussbericht <b>zu datieren und zu unterzeichnen</b> , um damit die Verantwortung für die Zuverlässigkeit der Daten zu übernehmen und anzugeben, inwieweit die Prüfung mit diesen Grundsätzen der Guten Laborpraxis übereinstimmt; ...	Unterschrift
Aufgaben des Qualitätssicherungspersonals	Das Qualitätssicherungspersonal hat zumindest ... eine dem Abschlussbericht beizufügende Erklärung abzufassen und zu <b>unterzeichnen</b> , aus der Art und Zeitpunkt der Inspektionen, die inspezierten Phasen der Prüfung sowie die Zeitpunkte, an denen der Leitung und dem Prüfleiter sowie gegebenenfalls einem Principal Investigator Inspektionsergebnisse berichtet wurden, hervorgehen. Weiterhin dient diese Erklärung als Bestätigung, dass der Abschlussbericht die Rohdaten widerspiegelt.	Unterzeichnen
Prüfplan	Vor Beginn jeder Prüfung muss ein schriftlicher Prüfplan vorliegen. Der Prüfplan muss vom Prüfleiter durch <b>datierte Unterschrift</b> genehmigt und vom Qualitätssicherungspersonal auf GLP-Konformität gemäß Abschnitt II 2.2. b) überprüft werden. Der Prüfplan muss auch von der Leitung der Prüfeinrichtung und dem Auftraggeber genehmigt werden, falls dies durch nationale Vorschriften oder Gesetze in dem Staat, in dem die Prüfung durchgeführt wird, gefordert wird.	Unterschrift
	Prüfplanänderungen müssen begründet und durch <b>datierte Unterschrift</b> des Prüfleiters genehmigt werden und sind gemeinsam mit dem Prüfplan aufzubewahren.	Unterschrift
Inhalt des Prüfplans	Das Datum der Genehmigung des Prüfplans durch <b>die Unterschrift</b> des Prüfleiters. Das Datum der Genehmigung des Prüfplans durch <b>die Unterschriften</b> der Leitung der Prüfeinrichtung und des Auftraggebers, falls dies durch nationale Vorschriften oder Gesetze in dem Staat, in dem die Prüfung durchgeführt wird, gefordert wird.	Unterschrift
Durchführung der Prüfung	Alle während der Prüfung erhobenen Daten sind durch die erhebende Person unmittelbar, unverzüglich, genau und leserlich aufzuzeichnen. Diese Aufzeichnungen sind <b>zu datieren und zu unterschreiben oder abzuzeichnen</b> .	Abzeichnen
	Daten, die als direkte Computereingabe entstehen, sind zur Zeit der Dateneingabe durch die dafür verantwortliche(n) Person(en) zu kennzeichnen. Computergestützte Systeme müssen so ausgelegt sein, dass jederzeit die Aufzeichnung eines vollständigen Audit Trails zur Verfügung steht, der sämtliche Datenänderungen anzeigt, ohne die Originaldaten unkenntlich zu machen. Alle Datenänderungen müssen mit der sie ändernden Person verknüpft werden können, z. B. durch die Verwendung von <b>mit Datum und Uhrzeit versehenen (elektronischen) Unterschriften</b> . Änderungen sind zu begründen.	Elektronische Unterschrift
Bericht über die Prüfergebnisse	Jeder Bericht eines an der Prüfung beteiligten Principal Investigators oder Wissenschaftlers ist von diesem <b>zu datieren und zu unterschreiben</b> .	Unterschrift

	Der Abschlussbericht muss vom Prüfleiter datiert und unterschrieben werden, um die Übernahme der Verantwortung für die Zuverlässigkeit der Daten zu dokumentieren. Des weiteren ist anzugeben, inwieweit die Prüfung mit diesen Grundsätzen der Guten Laborpraxis übereinstimmt.	Unterschrift
	Korrekturen und Ergänzungen eines Abschlussberichtes sind in Form von Nachträgen vorzunehmen. In Nachträgen sind die Gründe für die Korrekturen oder Ergänzungen deutlich darzulegen und vom Prüfleiter zu datieren und zu unterzeichnen.	Unterschrift

Tab. 6: OECD GLP-Konsensdokumente.

Absatz	Absatz aus OECD GLP-Konsensdokument Nr. 8	Gefordert
Die Rolle des Prüfleiters	Die Einhaltung der einschlägigen Vorschriften fällt ebenfalls in die Verantwortlichkeit des Prüfleiters. In dieser Funktion muss der Prüfleiter sicherstellen, dass die Prüfung in Übereinstimmung mit den GLP-Grundsätzen durchgeführt wird, deren Einhaltung er mit <b>seiner Unterschrift</b> im Abschlussbericht bestätigen muss.	Unterschrift
Die Verantwortlichkeiten des Prüfleiters	Der Prüfleiter muss den Prüfplan genehmigen, der vor Beginn der Prüfung mit datierter Unterschrift vorliegen muss. Dieses Dokument sollte die Ziele und den gesamten Verlauf der Prüfung klar definieren und angeben, wie diese erreicht werden sollen. Alle Änderungen zum Prüfplan müssen, wie oben beschrieben, genehmigt werden. ... Durch seine <b>datierte Unterschrift</b> auf dem Prüfplan übernimmt der Prüfleiter die Verantwortung für die Prüfung. Ab diesem Zeitpunkt (Beginn der Prüfung) wird der Prüfplan das offizielle Arbeitsdokument für diese Prüfung. Der Prüfleiter soll auch sicherstellen, dass der Prüfplan vom Auftraggeber und der Leitung der Prüfeinrichtung <b>unterschrieben</b> wird, soweit dies nationale Bestimmungen erforderlich machen.	Unterschrift
Abschlussbericht	Erst wenn der Prüfleiter sich davon überzeugt hat, dass der Bericht eine vollständige, wahrheitsgemäße und genaue Darstellung der Prüfung und ihrer Ergebnisse ist, soll er – und nur dann – den Abschlussbericht <b>unterschreiben und datieren</b> , um damit anzuzeigen, dass er die Verantwortung für die Zuverlässigkeit der Daten übernimmt. Es sollte auch angegeben werden, inwieweit die Prüfung mit den GLP-Grundsätzen übereinstimmt. Er sollte sich außerdem vergewissern, dass eine QS-Erklärung vorliegt und jede Abweichung vom Prüfplan dokumentiert wurde.	Unterschrift
Prüfplanänderung	Eine Prüfplanänderung sollte verfasst werden, um eine beabsichtigte Änderung im Prüfungsverlauf zu dokumentieren, die nach Beginn der Prüfung und vor Eintritt des Ereignisses vorgenommen wird. Eine Änderung kann auch als Ergebnis unerwarteter Ereignisse im Prüfungsverlauf, die wichtige Maßnahmen erfordern, verfasst werden. Die Prüfplanänderungen sollten vom Prüfleiter begründet, fortlaufend nummeriert und <b>datiert unterschrieben</b> allen Empfängern des Originalprüfplans zugeleitet werden.	Unterschrift
Rechtliche Stellung des Prüfleiters	Der Prüfleiter, der mit seiner <b>Unterschrift</b> im Abschlussbericht die Einhaltung der GLP-Grundsätze bestätigt, übernimmt die Verantwortung für die Durchführung der Prüfung gemäß den GLP-Grundsätzen und für die genaue Wiedergabe der Rohdaten im Abschlussbericht. Die gesetzliche Haftung des Prüfleiters wird jedoch nicht durch die OECD-GLP-Grundsätze, sondern durch die nationalen Gesetze und Rechtsvorschriften geregelt.	Unterschrift

Tab. 7: Neufassung Allgemeine Verwaltungsvorschrift (ChemVwV-GLP) zum Verfahren der behördlichen Überwachung der Einhaltung der Grundsätze der Guten Laborpraxis (ChemVwV-GLP) \*) vom 15. Mai 1997.

\*) Ist nicht aufgelöst.

Absatz	Absatz aus ChemVwV-GLP	Abzeichnen
Durchführung der Prüfung	<p>Zweck: Nachzuprüfen, ob schriftliche Prüfpläne vorliegen und ob Pläne und Durchführung der Prüfung mit den GLP-Grundsätzen übereinstimmen.</p> <p>Der Inspektor sollte sich vergewissern, dass</p> <ul style="list-style-type: none"> <li>• der Prüfplan vom Prüfleiter <b>abgezeichnet</b> wurde;</li> <li>• Änderungen zum Prüfplan vom Prüfleiter <b>abgezeichnet und datiert</b> sind;</li> <li>• (gegebenenfalls) das Datum registriert wurde, an dem der Auftraggeber dem Prüfplan zustimmte;</li> <li>• Messungen, Beobachtungen, Untersuchungen mit dem Prüfplan und einschlägigen Standardarbeitsanweisungen übereinstimmen;</li> <li>• die Ergebnisse dieser Messungen, Beobachtungen und Untersuchungen direkt, sofort, sorgfältig und leserlich aufgezeichnet, <b>unterzeichnet (oder abgezeichnet) und datiert</b> wurden;</li> <li>• etwaige Änderungen der Rohdaten, einschließlich der in Computern gespeicherten, frühere Eintragungen nicht unverständlich machen, der Grund für die Änderungen angegeben und so wohl die für die Änderung verantwortliche Person sowie das Datum, an dem dies vorgenommen wurde, ersichtlich ist;</li> <li>• durch Computer gewonnene oder gespeicherte Daten gekennzeichnet werden und dass die Verfahren geeignet sind, um diese Daten vor unerlaubten Änderungen oder Verlusten zu schützen; die im Rahmen der Prüfung eingesetzten Computersysteme zu verlässlich und genau sind und validiert worden sind;</li> <li>• alle in den Rohdaten verzeichneten unvorhergesehenen Ereignisse untersucht und bewertet wurden;</li> <li>• die Ergebnisse in den Prüfberichten (Zwischen- oder Abschlussberichten) folgerichtig und vollständig sind und die Rohdaten korrekt wiedergeben.</li> </ul>	Abzeichnen
Berichterstattung über die Ergebnisse der Prüfung	<p>Bei der Prüfung eines Abschlussberichtes sollte der Inspektor überprüfen, ob</p> <ul style="list-style-type: none"> <li>• der Prüfleiter diesen <b>mit Datum unterzeichnet</b> hat, womit die Übernahme der Verantwortung für die Qualität und Richtigkeit der Prüfung erklärt wird und bestätigt wird, dass die Prüfung in Übereinstimmung mit den GLP-Grundsätzen durchgeführt wurde;</li> <li>• Teilberichte, falls sie sich aus der Zusammenarbeit mit anderen Bereichen ergeben, von den dafür verantwortlichen Wissenschaftlern mit <b>Datum unterzeichnet</b> und in den Abschlussbericht einbezogen sind;</li> <li>• eine <b>unterzeichnete und datierte</b> Erklärung der Qualitätssicherung dem Bericht beiliegt; ...</li> </ul>	Unterschrift

Tab. 8: Arzneimittelgesetz (GCP).

Abschnitte	Absatz aus Arzneimittelgesetz (GCP)	Gefordert
AMG 1976 § 24 Sachverständigen- gutachten	Den nach § 22 Abs. 1 Nr. 15, Abs. 2 und 3 und § 23 erforderlichen Unterlagen sind Gutachten von Sachverständigen beizufügen, in denen die Kontrollmethoden, Prüfungsergebnisse und Rückstands-nachweisverfahren zusammengefasst und bewertet werden. Im Einzelnen muss aus den Gutachten insbesondere hervor-gehen ... Die Sachverständigen haben das Gutachten <b>eigenhändig zu unterschreiben</b> und dabei den <b>Ort und das Datum</b> der Erstellung des Gutachtens anzugeben.	Unterschrift

Tab. 9: Verordnung über die Anwendung der Guten Klinischen Praxis bei der Durchführung von klinischen Prüfungen mit Arznei-mitteln zur Anwendung am Menschen; 9. August 2004.

Abschnitte	Absatz aus Arzneimittelgesetz (GCP)	Gefordert
Abschnitt 1 Allgemeine Vorschriften GCP-V § 3 Begriffsbestimmungen, 2b	Einwilligung nach Aufklärung ist die Entscheidung über die Teil-nahme an einer klinischen Prüfung, die <b>in Schriftform abgefasst, datiert und unterschrieben werden muss</b> und nach ordnungs-gemäßer Unterrichtung über Wesen, Bedeutung, Tragweite und Risiken der Prüfung und nach Erhalt einer entsprechenden Doku-mentation freiwillig von einer Person, die ihre Einwilligung geben kann oder aber, wenn die Person hierzu nicht in der Lage ist, von ihrem gesetzlichen Vertreter getroffen wird. Kann die betreffende Person nicht schreiben, so kann in Ausnahmefällen eine münd-liche Einwilligung in Anwesenheit von mindestens einem Zeugen erteilt werden.	Unterschrift
Abschnitt 3 Genehmigung durch die Bundesober-behörde und Bewertung durch die Ethik-Kommis-sion GCP-V § 7 Antrag-stellung	Dem Antrag an die zuständige Ethik-Kommission und dem Antrag an die zuständige Bundesoberbehörde müssen vom Antragsteller die folgenden Angaben und Unterlagen beigefügt werden: 1. Kopie des Bestätigungsschreibens für die von der Europäischen Datenbank vergebene EudraCT-Nummer des Prüfplans, 2. vom Sponsor oder seinem Vertreter unterzeichnetes Begleit-schreiben in deutscher Sprache, das die EudraCT-Nummer, den Prüfplancode des Sponsors und den Titel der klinischen Prü-fung angibt, Besonderheiten der klinischen Prüfung hervorhebt und auf die Fundstellen der diesbezüglichen Informationen in den weiteren Unterlagen verweist, 3. vom Hauptprüfer oder vom Leiter der klinischen Prüfung sowie vom Sponsor oder seinem Vertreter <b>unterzeichneter Prüfplan</b> unter Angabe des vollständigen Titels und des Arbeitstitels der klinischen Prüfung, der EudraCT-Nummer, des Prüfplancodes des Sponsors, der Fassung und des <b>Datums</b> , ...	Unterschrift