

# Checkliste betreffend der technischen und organisatorischen Anforderungen an die elektronische Langzeitarchivierung

## 1. Document Retention Policy

Die Geschäftsleitung sorgt dafür, dass im Unternehmen bestimmt wird, welche Dokumente in welcher Form wie lange archiviert werden sollen

Sie berücksichtigt dabei

- a. die gesetzlichen Anforderungen an die kaufmännische Buchführung
- b. eventuell für den Geschäftsbereich des Unternehmens anwendbare Spezialgesetze
- c. Anforderungen an die Sicherung von Beweisen für eventuelle spätere Rechtsstreitigkeiten
- d. Bedürfnisse der internen Dokumentation und Information

Die Geschäftsleitung sorgt ausserdem für

- a. den Erlass der entsprechenden Weisungen im Unternehmen,
- b. die Schulung der Mitarbeitenden

## 2. Ordnungsgemässe Führung und Aufbewahrung der Bücher

Ordnungsmässigkeit ist eine besondere, gesetzlich geforderte Qualität der Buchführung, die es erlaubt, die Vermögenslage des Geschäfts und die mit dem Geschäft zusammenhängenden Schuld- und Forderungsverhältnisse sowie die Betriebsergebnisse der einzelnen Geschäftsjahre festzustellen. Dazu gehören die Grundsätze der **Richtigkeit, Vollständigkeit, Übereinstimmung der Regeln, Widerspruchsfreiheit, Kontinuität / Stetigkeit, Willkürfreiheit / Vergleichbarkeit, Prüfbarkeit**.

Die **Grundsätze der ordnungsgemässen Datenverarbeitung** sind **zusätzlich** und nur bei einer elektronischen oder vergleichbaren Führung und Aufbewahrung der Geschäftsbücher zu erfüllen.

Der dabei angesprochene **IT-Governance-Ansatz** geht von einem umfassenden Kontrollansatz aus, der alle Einflussfaktoren berücksichtigt!

Bei den Grundsätzen der ordnungsgemässen Datenverarbeitung ist die **Datensicherheit** angesprochen.

- Dies bedeutet, dass das verwendete Datenverarbeitungsverfahren Gewähr für eine fortlaufende, chronologische sowie lückenlose und systematische Erfassung sämtlicher Geschäftsvorfälle bieten muss.
- Es muss hard- und softwaremässig gewährleistet sein, dass bei der blossen Übertragung von originären Daten auf ein Speichermedium keine Bearbeitung derselben möglich ist, ohne dass dies bei entsprechender Überprüfung nachträglich festgestellt werden kann.
- Die Buchführungspflichtigen müssen periodisch Datensicherungsprozeduren zu den für die Buchführung relevanten Daten und Informationen durchführen. Ausserdem sollte eine Sicherungskopie dieser Daten erstellt und an einem anderen Standort aufbewahrt werden.
- Zugriffs- und Zugangskontrollen sind vorzusehen.
- Um die Lesbarkeit der Daten zu sichern, empfiehlt sich die Vornahme folgender Massnahmen:
  - Periodisches Umkopieren der Daten auf neue Datenträger.
  - Periodische Konvertierung oder Migration, d.h. Übertragung der Daten in ein neues Datenformat.
  - Emulation, d.h. Erhaltung der zum Lesen der Daten benötigten Systeme indem man diese letzteren auf neueren Systemen künstlich nachbaut.
- Die Speicherung der Daten in einem Format, das auf allgemein anerkannten Standards und öffentlich zugänglichen Spezifikationen basiert.
- Das Risiko der Unauffindbarkeit muss durch das Führen eines systematischen Verzeichnisses über die gespeicherten Datenbestände und Datenverarbeitungssysteme eingeschränkt werden.
- Um das Risiko der Vernichtung oder des Diebstahls der Datenträger rechtsgenügend auszuschliessen oder zu vermindern, sind diese letzterwähnten in gegen Einbruch, Feuer, Feuchtigkeit, Magnetfelder etc. genügend gesicherten Räumen bzw. Tresoren aufzubewahren.

### 3. Integrität

Die Geschäftsbücher müssen so geführt und aufbewahrt und die Buchungsbelege und die Geschäftskorrespondenz müssen so erfasst und aufbewahrt werden, dass sie nicht geändert werden können, ohne dass sich dies feststellen lässt.

Es werden keine höheren Anforderungen gestellt als an Papierdokumente und es **wird keine absolute Unabänderbarkeit** der Geschäftsbücher verlangt.

Verlangt wird, dass nachträgliche Änderungen auch feststellbar sind.

Dies kann z.B. durch den Einsatz der digitalen Signatur erfolgen.

### 4. Dokumentationspflichten

Die Dokumentationspflichten stellen sicher, dass die aufbewahrten Geschäftsdokumente auch verstanden werden können. Dazu sind die für das Verständnis der Unterlagen notwendigen Metadaten zu archivieren.

### 5. Allgemeine Sorgfaltspflichten

Die Geschäftsbücher, die Buchungsbelege und die Geschäftskorrespondenz sind sorgfältig, geordnet und vor schädlichen Einwirkungen geschützt aufzubewahren.

Um das Risiko der Vernichtung oder des Diebstahls der Datenträger rechtsgenügend auszuschliessen oder zu vermindern, sind diese letzterwähnten in gegen Einbruch, Feuer, Feuchtigkeit, Magnetfelder etc. genügend gesicherten Räumen bzw. Tresoren aufzubewahren (Überschneidung mit dem Grundsatz der Datensicherheit, gilt aber auch für Aufbewahrung in Papierform).

### 6. Verfügbarkeit

Die Geschäftsbücher, die Buchungsbelege und die Geschäftskorrespondenz müssen so aufbewahrt werden, dass sie bis zum Ende der Aufbewahrungsfrist von einer berechtigten Person innert angemessener Frist eingesehen und geprüft werden können.

Was genau unter angemessener Frist zu verstehen ist, wird erst die Praxis zeigen. Zudem ist bei einer elektronischen Führung und Aufbewahrung der Geschäftsdokumente auch die Aufbewahrung der Verifikationsdaten erforderlich!

Daraus folgt, dass bei einem Personalwechsel das Know-how betreffend der angewandten Technik und Verfahren weitergegeben werden muss. Um dies sicherzustellen, müssen ausreichende Dokumentationen vorhanden sein (Art. 4) und das Personal muss geschult werden.

Verlangt eine berechtigte Person Einsicht, dann muss ihr z.B. ein Ausdruck in Papierform ausgehändigt werden.

### 7. Organisation

Archivierte Informationen sind von aktuellen Informationen zu trennen bzw. so zu kennzeichnen, dass eine Unterscheidung möglich ist. Die Verantwortung für die archivierten Informationen ist klar zu regeln und zu dokumentieren.

Auf archivierte Daten muss innert nützlicher Frist zugegriffen werden können. Eine Vermischung von Archiv und aktuellen Daten ist laut Gesetz nicht zulässig. Die organisatorische Trennung ist auch Voraussetzung dafür, dass die Verantwortung für diese Informationen sauber geregelt werden kann.

Die Informationen sind systematisch zu inventarisieren und vor unbefugtem Zugriff zu schützen. Zugriffe und Zutritte sind aufzuzeichnen. Diese Aufzeichnungen unterliegen derselben Aufbewahrungspflicht wie die Datenträger.

Dies ist eine wesentliche Voraussetzung dafür, dass die Daten verfügbar sind und innert angemessener Frist darauf zugegriffen werden kann und sie verstanden werden können.

Die Aufzeichnung der Zugriffe und Zutritte zum Archiv dient der Datensicherheit. Diese Vorschrift ist allerdings auf alle Arten der Aufbewahrung anwendbar.

Quelle: Frau mag. iur. Maria Winkler, IT & Law Consulting GmbH

Mehr Informationen zu diesem Thema finden Sie unter [www.vereon.ch/rea](http://www.vereon.ch/rea)

## 8. Zulässige Informationsträger

Zur Aufbewahrung von Unterlagen sind zulässig:

- a. unveränderbare Informationsträger, namentlich Papier, Bildträger und unveränderbare Datenträger;
- b. veränderbare Informationsträger, wenn:

technische Verfahren zur Anwendung kommen, welche die Integrität der gespeicherten Informationen gewährleisten (z.B. digitale Signaturverfahren),

der Zeitpunkt der Speicherung der Informationen unverfälschbar nachweisbar ist (z.B. durch „Zeitstempel“),

die zum Zeitpunkt der Speicherung bestehenden weiteren Vorschriften über den Einsatz der betreffenden technischen Verfahren eingehalten werden, und

die Abläufe und Verfahren zu deren Einsatz festgelegt und dokumentiert sowie die entsprechenden Hilfsinformationen (wie Protokolle und Log files) ebenfalls aufbewahrt werden.

Die Verordnung ist technikneutral verfasst, sie lässt dadurch Raum für künftige technische Entwicklungen (z.B. kristalline Medien). Es wird der Praxis überlassen festzulegen, welcher Datenträger als unveränderbar gilt. Grundsätzlich wird bei der Beantwortung dieser Frage immer auf den **aktuellen Stand der Technik** abzustellen sein.

Die GeBüV verlangt die Sicherstellung der Integrität der Daten durch zusätzliche **technische** Sicherungsmassnahmen. Ausschliesslich organisatorische Massnahmen (Zugriffe und Zutritte rigoros regeln und überwachen) sind nach dem Wortlaut ausgeschlossen.

Die digitale Signatur wird nur beispielsweise erwähnt. Zudem ist nicht erforderlich, dass die qualifizierte digitale Signatur verwendet wird, sodass die Verwendung des Verfahrens allein ausreichen müsste.

Es ist zu beachten, dass je nach Art des verwendeten Zeitstempeldienstes ein mehr oder minder grosser Beweiswert gegeben ist.

## 9. Archivierungskonzept

Die Informationsträger sind regelmässig auf ihre Integrität und Lesbarkeit zu prüfen.

Die Daten können in andere Formate oder auf andere Informationsträger übertragen werden (Datenmigration), wenn sichergestellt wird, dass:

- a. die Vollständigkeit und die Richtigkeit der Informationen gewährleistet bleiben; und
- b. die Verfügbarkeit und die Lesbarkeit den gesetzlichen Anforderungen weiterhin genügen.

Die Übertragung von Daten von einem Informationsträger auf einen anderen ist zu protokollieren. Das Protokoll ist zusammen mit den Informationen aufzubewahren.

Ein Archivierungskonzept hat sicherzustellen, dass diese vorgeschriebenen Kontrollen regelmässig durchgeführt werden.

Mit dieser Bestimmung trägt der Gesetzgeber der raschen technischen Entwicklung Rechnung. Die Migration in andere Formate oder auf andere Informationsträger ist ausdrücklich zulässig.

Allerdings ist dabei zu beachten, dass dabei bei digital signierten Daten die Signatur gebrochen wird. Die Nutz- und die Signierdaten des Originaldokuments müssen gemeinsam mit dem Protokoll aufzubewahren.

## Einige Auswahlkriterien für ein elektronisches Archivsystem

1. Verwendung von standardisierten Datenformaten	<p>Erleichtert die Migration von Daten</p> <p>Erhöht die Aussicht, dass die technischen Komponenten zur Visualisierung während des gesamten Aufbewahrungszeitraumes verfügbar sind</p> <p>Der Anwender ist dadurch weniger von einem Anbieter abhängig, was bei einer derart weitreichenden und langfristigen Investitionsentscheidung ausschlaggebend sein kann</p> <p>Zur Zeit wird insbesondere bei eGovernment-Lösungen der Austausch von Daten im XML-Format favorisiert!</p>
2. Unterstützung von nationalen und internationalen Signatursystemen	<p>Auch wenn die Verbreitung der digitalen Signatur noch nicht gesichert ist, kann die Unterstützung der elektronischen Signatur doch als eine der Basisvoraussetzungen für elektronische Langzeitarchivierungssysteme bezeichnet werden.</p>
3. Unterstützung von nationalen und internationalen Zeitstempeldiensten	<p>Es ist darauf zu achten, dass dem Kunden immer die sicherste Variante zu empfehlen ist!</p>

4. Berücksichtigung der Möglichkeit einer Signaturerneuerung	Bei Unsicherwerden der verwendeten Schlüssellängen muss der Kunde die verwendete Signatur gegebenenfalls erneuern. Das System sollte den Kunden dabei unterstützen.
5. Archivierung der Verifikationsdaten	Es sollte berücksichtigt werden, dass die Verifikationsdaten für die elektronische Signatur (Zertifikate, Zeitstempel, etc.) während der gesamten Aufbewahrungsdauer archiviert werden müssen
6. Unterstützung der Dokumentationspflichten	Die gesetzeskonforme elektronische Archivierung ist nur unter Einhaltung zahlreicher Dokumentationspflichten möglich. Das System sollte den Kunden bei der Erfüllung dieser Dokumentationspflichten durch die Integration entsprechender Tools unterstützen.
7. Trennung zwischen Archivdaten und aktuellen Daten	Diese Trennung ist im Gesetz ausdrücklich vorgesehen und eine grundlegende Voraussetzung für die Regelung der Zuständigkeiten für archivierte Daten
8. Berücksichtigung der datenschutzrechtlichen Anforderungen	Einsichtsrecht des Betroffenen muss gewährleistet werden Löschung und/oder Berichtigung einzelner Dokumente muss möglich sein, ohne dass die Beweiskraft der übrigen Dokumente schwindet
9. Sicherstellung der Wartung und Weiterentwicklung	Bereitschaftszeiten, Reaktionszeiten, Kündigungsfristen und Kündigungstermine müssen den Bedürfnissen des Unternehmens entsprechen Escrow Agreements stellen den Zugriff auf den Sourdecode (z.B. im Fall des Konkurses des Anbieters) sicher

Quelle: Frau mag. iur. Maria Winkler, IT & Law Consulting GmbH

Mehr Informationen zu diesem Thema finden Sie unter [www.vereon.ch/rea](http://www.vereon.ch/rea)