

**Grundsätze ordnungsgemäßer Buchführung bei Einsatz von IT-Verfahren im Haushalts-,
Kassen- und Rechnungswesen
(GoBIT-HKR)**

Inhalt

1 Anwendungsbereich, Allgemeines.....	1
2 Verantwortlichkeit.....	1
3 Allgemeine Anforderungen.....	1
4 Belegfunktion.....	2
5 Internes Kontrollsystem (IKS)	3
6 Aufbewahrung von elektronischen Unterlagen.....	4

1

Anwendungsbereich, Allgemeines

Die Abläufe im Haushalts-, Kassen- und Rechnungswesen gem. Nr. 6.1.1 zu § 79 werden zunehmend ganz oder teilweise unter Einsatz von automatisierten, integrierten IT-Verfahren für die Bewirtschaftung, die Buchführung und die Rechnungslegung abgebildet. Hierunter sind solche Verfahren zu verstehen, bei denen alle Arbeitsschritte grundsätzlich ohne Unterbrechung auf elektronischem Wege ablaufen. Das ist auch der Fall, wenn Arbeitsschritte in einem abgesetzten Verfahren (Vorverfahren) bearbeitet und deren Ergebnisse elektronisch in ein zentrales IT-Verfahren für die Bewirtschaftung, Buchführung und Rechnungslegung übergeben werden.

Darüber hinaus werden im Haushalts-, Kassen- und Rechnungswesen die aufbewahrungspflichtigen Unterlagen zunehmend in elektronischer Form aufbewahrt.

2

Verantwortlichkeit

Für die Einhaltung der nachfolgenden Bestimmungen beim Einsatz von IT-Verfahren gemäß Nr. 1 ist das für den Einsatz des IT-Verfahrens zuständige Ressort verantwortlich, dessen Einzelplan oder Teile davon mit dem IT-Verfahren bewirtschaftet werden. Dies gilt auch bei einer teilweisen oder vollständigen organisatorischen und technischen Auslagerung der Buchführung und Rechnungslegung auf Dritte. Von der Leitung des einsetzenden Ressorts ist die verantwortliche Organisationseinheit zu bestimmen und dem Ministerium der Finanzen mitzuteilen

Für die Verfahrensabläufe in der einsetzenden Dienststelle ist die jeweilige Dienststelle verantwortlich. Dies beinhaltet die Gewährleistung der Ordnungsmäßigkeit der in den IT-Verfahren entstandenen bzw. bearbeiteten elektronischen Unterlagen einschließlich des ordnungsgemäßen Einsatzes des Verfahrens, soweit es die Verfahrensabläufe in der Dienststelle betrifft. Von der Leitung der einsetzenden Dienststelle ist die verantwortliche Organisationseinheit zu bestimmen und dem für den Einsatz des IT-Verfahrens zuständigen Ressort mitzuteilen.

3

Allgemeine Anforderungen

Für Verfahren nach Nr. 6.1.1.1 bis 6.1.1.4 zu § 79 gelten die Grundsätze nach § 238 Abs. 1 und § 239 Absätze 2 und 3 des Handelsgesetzbuches. Neben diesen rechtlichen Grundsätzen ist die

Einhaltung nachfolgender allgemeiner Anforderungen Voraussetzung für die Ordnungsmäßigkeit eines IT-gestützten Verfahrens für die Bewirtschaftung, die Buchführung und die Rechnungslegung.

3.1

Vertraulichkeit

Es muss sichergestellt werden, dass Daten nicht unberechtigt weitergegeben oder veröffentlicht werden.

3.2

Integrität

Die Daten, die IT-Infrastruktur und die IT-Anwendungen müssen vollständig und richtig zur Verfügung stehen und vor Manipulation und ungewollten oder fehlerhaften Änderungen geschützt sein. Die Ordnungsmäßigkeit der IT-gestützten Rechnungslegung setzt voraus, dass neben den Daten und IT-Anwendungen auch die IT-Infrastruktur nur in einem festgelegten Zustand eingesetzt wird und nur autorisierte Änderungen zugelassen werden.

3.3

Verfügbarkeit

Zur Aufrechterhaltung des Dienstbetriebs ist die Verfügbarkeit der IT-Infrastruktur, der IT-Anwendungen mit den Daten und der IT-Organisation durch die zuständige Stelle zu gewährleisten. Maßnahmen zur Sicherung der Verfügbarkeit sind erforderlich, um den Anforderungen nach Lesbarmachung der Buchführung gerecht zu werden.

3.4

Autorisierung

Es muss sichergestellt sein, dass nur im Voraus festgelegte Personen auf Daten zugreifen können (autorisierte Personen) und dass nur sie die für das IT-Verfahren definierten Rechte wahrnehmen können. Diese Rechte betreffen insbesondere das Lesen, Erfassen, Ändern und Löschen von Daten oder die Administration eines IT-Verfahrens. Geeignete Verfahren hierfür sind physische und logische Zugriffsschutzmaßnahmen. Organisatorische Regelungen und technische Systeme zum Zugriffsschutz sind die Voraussetzung zur Umsetzung der erforderlichen Funktionstrennungen.

3.5

Authentizität

Es muss sichergestellt sein, dass die in das IT-Verfahren eingestellten Daten eines Geschäftsvorfalles einem Verursacher eindeutig zugeordnet werden können.

3.6

Verbindlichkeit

Es ist sicherzustellen, dass das IT-Verfahren die von der zuständigen Stelle gewollten Rechtsfolgen bindend herbeiführt.

4

Belegfunktion

4.1

Belegverarbeitung

4.1.1

Aus der Verfahrensdokumentation gemäß Nr. 6.1.2 zu § 79 muss ersichtlich sein, wie die elektronischen Belege erfasst, empfangen, verarbeitet, ausgegeben und aufbewahrt werden.

4.1.2

Eingehende elektronische Unterlagen sind im Rahmen der sachlichen Feststellung auf Authentizität (Nr. 3.5) zu prüfen.

4.2

Belegsicherung

4.2.1

Die Belege sind unmittelbar nach Eingang oder Entstehung gegen Verlust zu sichern (Nr. 6.1 und 6.2).

4.2.2

Zur Sicherung der Beweiskraft sind Belege und Buchungen so zu kennzeichnen, dass sie gegenseitig eindeutig zugeordnet werden können.

4.2.3

Liegen den Buchungen automatisierte Berechnungsprozesse teilweise oder vollständig zu Grunde, sind sie in der Verfahrensdokumentation zu beschreiben. Änderungen der automatisierten Berechnungsprozesse sind nur mittels eines autorisierten Änderungsverfahrens zulässig.

5

Internes Kontrollsystem (IKS)

Als IKS wird grundsätzlich die Gesamtheit aller aufeinander abgestimmten und miteinander verbundenen Kontrollen, Maßnahmen und Regelungen bezeichnet, die die Einhaltung der Ordnungsvorschriften sicherstellt.

5.1

Einhaltung der Ordnungsvorschriften

Für die Einhaltung der Ordnungsvorschriften (Nr. 3) sind Kontrollen einzurichten, auszuüben und zu protokollieren. Hierzu gehören insbesondere:

5.1.1

Zugangs- und Zugriffsberechtigungskontrollen auf Basis entsprechender Zugangs- und Zugriffsberechtigungskonzepte,

5.1.2

Kontrollen über die Einhaltung der Funktionstrennung

5.1.3

Erfassungs- und Abstimmungskontrollen (z. B. Fehlerhinweise, Plausibilitätsprüfungen),

5.1.4

Verarbeitungskontrollen,

5.1.5

Kontrollen zur Einhaltung der Schutzmaßnahmen gegen die beabsichtigte und unbeabsichtigte Verfälschung von Programmen und elektronischen Unterlagen und

5.1.6

Kontrollen, die sicherstellen, dass Änderungen an automatisierten Berechnungsprozessen nur mittels autorisierter Änderungsverfahren durchgeführt werden.

5.2

Anlassbezogene Prüfungen

Im Rahmen eines IKS muss auch anlassbezogen (z. B. Systemwechsel) geprüft werden, ob das eingesetzte IT-Verfahren dem dokumentierten Verfahren entspricht.

6

Aufbewahrung von elektronischen Unterlagen

6.1

Allgemeine Aufbewahrungspflichten

Der sachliche Umfang der Aufbewahrungspflicht ergibt sich aus Nr. 4.7 zu § 79.

6.2

Besondere Aufbewahrungspflichten

6.2.1

Bei den elektronischen Unterlagen ist im Hinblick auf deren Aufbewahrungspflicht auf ihren Inhalt abzustellen. So ist z. B. eine E-Mail in elektronischer Form aufbewahrungspflichtig, wenn sie sich als originäre begründende Unterlage darstellt. Dient eine E-Mail nur als „Transportmittel“, z. B. für einen angehängten elektronischen Beleg, und enthält darüber hinaus keine weitergehenden aufbewahrungspflichtigen Informationen, so ist sie nicht aufbewahrungspflichtig, wohl aber der angehängte elektronische Beleg.

6.2.2

Bei elektronischen Unterlagen ist ihr Eingang, ihre weitere Verarbeitung sowie ihre Aufbewahrung zu protokollieren. Die elektronischen Bearbeitungsvorgänge sind mit der elektronischen Unterlage zu speichern, damit die Nachvollziehbarkeit und Prüfbarkeit des Originalzustands und seiner Ergänzungen gewährleistet ist. Dabei muss sichergestellt sein, dass die beteiligten und verantwortlichen Personen und der Umfang der von ihnen jeweils wahrgenommenen Verantwortung eindeutig, dauerhaft und unveränderlich unter Angabe des Datums und ggf. der Uhrzeit systemseitig revisionssicher dokumentiert werden und die Zugehörigkeit der einzelnen Unterlagen zu einem Geschäftsvorfall erkennbar bleibt.

6.2.3

Sind aufbewahrungspflichtige elektronische Unterlagen in einem IT-Verfahren entstanden oder eingegangen, so sind diese Daten in der Form der Erstellung oder der Übernahme unveränderbar aufzubewahren und dürfen vor Ablauf der Aufbewahrungsfrist nicht gelöscht werden. Dies gilt unabhängig davon, ob die Aufbewahrung im Produktivsystem oder durch Auslagerung in ein Archivsystem erfolgt. Es ist sicherzustellen, dass die elektronischen Unterlagen innerhalb der Aufbewahrungszeit auch nach einem Wechsel der zum Zeitpunkt der Speicherung eingesetzten IT-Verfahren lesbar gemacht und ausgewertet werden können.

6.2.4

Elektronische Unterlagen sind in einem sicheren Verfahren gegen Veränderung, Verlust, Beschädigung und den Zugriff Unbefugter geschützt aufzubewahren. Es muss sichergestellt sein, dass die Verfügbarkeit, die Lesbarkeit und die maschinelle Auswertbarkeit der Unterlagen während der Dauer der Aufbewahrung nicht beeinträchtigt werden. Für Zwecke der Aufbewahrung von elektronischen Unterlagen ist eine digitale Signatur nicht erforderlich.

6.2.5

Eine elektronische Unterlage muss innerhalb einer angemessenen Frist lesbar gemacht und zur Verfügung gestellt werden können. Es ist sicherzustellen, dass die elektronische Unterlage mit weiteren dazugehörigen Unterlagen zusammengeführt werden kann. Dies gilt für die gesamte Aufbewahrungsfrist.

6.3

Prüfbarkeit der aufbewahrungspflichtigen elektronischen Unterlagen

Die elektronischen Unterlagen müssen für die Rechnungsprüfung und für die Aufgaben nach § 9 LHO auch maschinell auswertbar sein.

6.4

Elektronische Erfassung von Unterlagen in Papierform

6.4.1

Unterlagen in Papierform werden durch den Scanvorgang in elektronische Unterlagen umgewandelt. Mit dem Scanvorgang wechselt die Belegfunktion von der Unterlage in Papierform zu der elektronischen Unterlage. Es muss bei dem Scanvorgang sichergestellt werden, dass die gescannte Unterlage mit dem Original übereinstimmt und der Zusammenhang bei mehrseitigen Vorlagen gewahrt bleibt.

6.4.2

Die Unterlagen in Papierform dürfen nach dem fehlerfreien Scanvorgang vernichtet werden. Dies gilt nicht, wenn Rechtsvorschriften oder andere zwingende Gründe dem entgegenstehen. Die weitere Bearbeitung darf nur noch mit der elektronischen Unterlage erfolgen. Werden die Unterlagen in Papierform nicht vernichtet, so dürfen deshalb auf ihnen keine Bemerkungen, Ergänzungen usw. angebracht werden, die auf der elektronischen Unterlage nicht enthalten sind. Soweit aus zwingenden Gründen nach dem Scanvorgang dennoch eine weitere Vorgangsbearbeitung der Unterlage in Papierform erfolgt und hierbei Bemerkungen, Ergänzungen usw. auf ihr angebracht werden, muss nach Abschluss der Bearbeitung die Unterlage erneut eingescannt und ein Bezug zum ersten Scanobjekt in Form einer Historie hergestellt werden.

6.4.3

Die für den Scan-Vorgang zuständige Dienststelle hat, unter Beteiligung des oder der Beauftragten für den Haushalt, eine Dienstanweisung zu erstellen, die unter anderem regelt,

6.4.3.1

wer nach dem Berechtigungskonzept scannen darf,

6.4.3.2

zu welchem Zeitpunkt gescannt wird (z. B. beim Posteingang, während oder nach Abschluss der Vorgangsbearbeitung),

6.4.3.3

welche Unterlagen gescannt werden,

6.4.3.4

welche Unterlagen in Papierform nach dem Scanvorgang nicht vernichtet werden dürfen,

6.4.3.5

wie die Qualitätskontrolle auf Lesbarkeit und Vollständigkeit erfolgt,

6.4.3.6

wie die elektronische Unterlage einem Geschäftsvorfall zugeordnet wird,

6.4.3.7

wie Fehler protokolliert werden und

6.4.3.8

wie mit fehlerhaften Scan-Ergebnissen umzugehen ist.