Anlage 32a
zu VV Nr. 6 zu den §§ 70 bis 72 und 75 bis 80 LHO

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

Inhalt:

1 Anwendungsbereich

1.1 Allgemeines

Die Abläufe im Haushalts-, Kassen- und Rechnungswesen gemäß VV Nr. 6.1.1 zu den §§ 70 bis 72 und 75 bis 80 werden zunehmend ganz oder teilweise unter Einsatz von automatisierten, integrierten IT-gestützten Buchführungs- und Rechnungslegungssysteme 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 das zentrale automatisierte HKR-Verfahren übergeben werden.

1.2 Elektronische Unterlagen

Elektronische Unterlagen sind alle Unterlagen gemäß VV Nr. 4.7 zu den §§ 70 bis 72 und 75 bis 80.

2 Verantwortlichkeit

Für die Einhaltung der nachfolgenden Bestimmungen für den Einsatz eines Verfahrens nach Nummer 1 ist die oder der Beauftragte für den Haushalt der obersten Behörde verantwortlich, die für den Einsatz des Verfahrens zuständig ist. Dies beinhaltet die Gewährleistung der Ordnungsmäßigkeit der elektronischen Unterlagen nach Nummer 1.1 einschließlich der eingesetzten Verfahren. Dies gilt auch bei einer teilweisen oder vollständigen organisatorischen und technischen Auslagerung der Buchführung und Rechnungslegung auf Dritte. Die oder der Beauftragte für den Haushalt der obersten Behörde kann ihre oder seine Verantwortlichkeit an eine andere Beauftragte oder einen anderen Beauftragten für den Haushalt übertragen.

3 Allgemeine Anforderungen

Neben den rechtlichen Grundsätzen gemäß VV Nr. 6.1.1 zu den §§ 70 bis 72 und 75 bis 80 ist die Sicherstellung und Einhaltung nachfolgender allgemeiner Anforderungen Voraussetzung für die Ordnungsmäßigkeit eines IT-gestützten Buchführungs- und Rechnungslegungssystems.

3.1 Vertraulichkeit

Vertraulichkeit verlangt, dass Daten nicht unberechtigt weitergegeben oder veröffentlicht werden.

3.2 Integrität

Integrität von IT-Verfahren ist gegeben, wenn die Daten und die IT-Infrastruktur sowie die IT-Anwendungen vollständig und richtig zur Verfügung stehen und vor Manipulation und ungewollten oder fehlerhaften Änderungen geschützt sind. Organisatorische Maßnahmen sind geeignete Test- und Freigabe-verfahren. 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

Verfügbarkeit verlangt zum einen, dass die zuständige Stelle zur Aufrechterhaltung des Dienstbetriebs die erforderliche Nutzung der IT-Infrastruktur, der IT-Anwendungen mit den Daten und der IT-Organisation gewährleistet. Zum anderen sind Maßnahmen zur Sicherung der Verfügbarkeit erforderlich, um den Anforderungen nach Lesbarmachung der Buchführung gerecht zu werden.

3.4 Autorisierung

Autorisierung bedeutet, dass nur im Voraus festgelegte Personen und andere IT-Verfahren auf Daten zugreifen können und 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. Dadurch soll ausschließlich die genehmigte Abbildung von Geschäftsvorfällen im Verfahren gewährleistet werden. 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

Authentizität ist gegeben, wenn ein Geschäftsvorfall einem Verursacher eindeutig zuzuordnen ist.

3.6 Verbindlichkeit

Verbindlichkeit ist die Eigenschaft von IT-gestützten Verfahren, gewollte Rechtsfolgen bindend herbeizuführen.

4 Belegfunktion

4.1 Belegverarbeitung

Aus der Verfahrensdokumentation (VV Nr. 6.2 zu den §§ 70 bis 72 und 75 bis 80) muss ersichtlich sein, wie die elektronischen Belege erfasst, empfangen, verarbeitet, ausgegeben und aufbewahrt werden (Nummern 6.1 und 6.2).

4.2 Belegsicherung

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

4.2.2 Zur Sicherung der Beweiskraft nach VV Nr. 4.1.1 zu den §§ 70 bis 72 und 75 bis 80 sind Belege und Buchungen so zu kennzeichnen, dass sie gegenseitig eindeutig zugeordnet werden können.

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

5 Internes Kontrollsystem (IKS)

5.1 Einhaltung der Ordnungsvorschriften

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

5.1.1 Zugangs- und Zugriffsberechtigungskontrollen auf Basis entsprechender Zugangs- und Zugriffsberechtigungskonzepte (zum Beispiel spezifische Zugangs- und Zugriffsberechtigungen),

5.1.2 Funktionstrennungen,

5.1.3 Erfassungskontrollen (Fehlerhinweise, Plausibilitätsprüfungen),

5.1.4 Abstimmungskontrollen bei der Dateneingabe,

5.1.5 Verarbeitungskontrollen,

5.1.6 Schutzmaßnahmen gegen die beabsichtigte und unbeabsichtigte Verfälschung von Programmen und elektronischen Unterlagen und

5.1.7 Änderungen von automatisierten Berechnungsprozessen nur mittels autorisierter Änderungsverfahren.

5.2 Anlassbezogene Prüfungen

Im Rahmen eines funktionsfähigen IKS muss auch anlassbezogen (zum Beispiel Systemwechsel) geprüft werden, ob das eingesetzte IT-Verfahren tatsächlich dem dokumentierten Verfahren entspricht (VV Nr. 6.2 zu den §§ 70 bis 72 und 75 bis 80).

6 Aufbewahrung von elektronischen Unterlagen

6.1 Allgemeine Aufbewahrungsplichten

Der sachliche Umfang der Aufbewahrungspflicht ergibt sich aus VV Nr. 4.7 zu den §§ 70 bis 72 und 75 bis 80.

6.2 Besondere Aufbewahrungspflichten

6.2.1 Bei elektronischen Unterlagen ist ihr Eingang, ihre Aufbewahrung und gegebenenfalls Konvertierung sowie die weitere Verarbeitung zu protokollieren. Dabei muss sichergestellt sein, dass die beteiligten Personen und der Umfang der von ihnen jeweils wahrgenommenen Verantwortung eindeutig, dauerhaft und unveränderlich unter Angabe des Datums und gegebenenfalls der Uhrzeit systemseitig revisionssicher dokumentiert wird und der Zusammenhang der einzelnen Unterlagen zu einem Geschäftsvorfall gewahrt bleibt.

6.2.2 Es muss sichergestellt sein, dass ein sachverständiger Dritter innerhalb angemessener Zeit prüfen kann. Die Unterlagen sind so geordnet aufzubewahren, dass innerhalb einer angemessenen Frist einzelne Unterlagen zur Verfügung stehen.

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 unveränderbar, gegen Verlust, Beschädigung und den Zugriff Unbefugter aufzubewahren. Es muss sichergestellt sein, dass die Haltbarkeit, die Lesbarkeit und die maschinelle Auswertbarkeit der Unterlagen während der Dauer der Aufbewahrung nicht beeinträchtigt werden. Bei der Aufbewahrung von elektronischen Unterlagen ist eine elektronische Signatur nicht erforderlich.

6.2.5 Eingehende elektronische Unterlagen sind im Rahmen der sachlichen Feststellung auf Integrität (Nummer 3.2) und Authentizität (Nummer 3.5) zu prüfen. Bei den elektronischen Unterlagen ist auf deren Inhalt abzustellen. So ist zum Beispiel eine E-Mail in elektronischer Form aufbewahrungspflichtig, wenn sie sich als originäre begründende Unterlage darstellt. Dient eine E-Mail nur als „Transportmittel“, zum Beispiel für eine angehängte elektronische Rechnung, und enthält darüber hinaus keine weitergehenden aufbewahrungspflichtigen Informationen, so ist diese nicht aufbewahrungspflichtig.

6.2.6 Eine elektronische Unterlage ist so zu kennzeichnen, dass sie jederzeit innerhalb einer angemessenen Frist lesbar gemacht werden kann. Es ist sicherzustellen, dass die elektronische Unterlage unter dem Kennzeichen verwaltet und mit weiteren dazugehörigen Unterlagen zusammengeführt werden kann. Dies gilt für die gesamte Aufbewahrungsfrist.

6.2.7 Die elektronischen Bearbeitungsvorgänge sind zu protokollieren und mit der elektronischen Unterlage zu speichern, damit die Nachvollziehbarkeit und Prüfbarkeit des Originalzustands und seiner Ergänzungen gewährleistet ist.

6.2.8 Bei Einsatz von Kryptografietechniken brauchen nur die entschlüsselten elektronischen Unterlagen aufbewahrt zu werden.

6.2.9 Die Aufbewahrung elektronischer Unterlagen bei Bargeschäften regelt das für Finanzen zuständige Ministerium.

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. Es muss dabei sichergestellt werden, dass das Original mit der gescannten Unterlage übereinstimmt und der Zusammenhang der einzelnen Unterlagen gewahrt bleibt.

6.4.2 Die Unterlagen in Papierform dürfen nach dem fehlerfreien Scanvorgang vernichtet werden und die weitere Bearbeitung darf nur noch mit der elektronischen Unterlage erfolgen. Dies gilt nicht, wenn Rechtsvorschriften oder andere zwingende Gründe dem entgegenstehen.

6.4.3 Das Verfahren muss dokumentiert werden. Die zuständige Stelle muss eine Dienstanweisung erstellen, die unter anderem regelt,

6.4.3.1 wer nach dem Berechtigungskonzept scannen darf,

6.4.3.2 zu welchem Zeitpunkt gescannt wird (zum Beispiel 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 und

6.4.3.7 wie Fehler protokolliert werden.